Weekly Security Articles 29-December-2022

Contribution Managers:

Christopher Sundberg

Kirsten Koepsel

Vanessa DiMase

Daniel DiMase

Please Take our On-Line Survey

We would like to keep the Weekly Security Articles of Interest of interest relevant and timely. Please take a few minutes to answer our brief survey.

Thank you!

Link to Survey: https://forms.gle/L95wrYfa5sh3cZRQ8

NOTE: The results of the survey will be used to determine direction of the weekly Security Articles of Interest.

The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

TLP Definition: https://www.cisa.gov/tlp

Contents

The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

If you have publicly available contribution that you would like to share that may be added to this weekly report in the future, please send them to daniel.dimase@aerocyonics.com *along with the URL for the document.*

The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Events - Online

Initial Meeting of the IoT Advisory Board

Source: https://www.nist.gov/news-events/events/2023/01/initial-meeting-iot-advisory-board

January 18-19, 2023

Cybersecurity Standardisation Conference 2023

Source: https://www.enisa.europa.eu/events/cybersecurity_standardisation_2023

February 7, 2023

Events - In-person

Convene: Clearwater 2023

Source: https://staysafeonline.org/programs/events/convene-clearwater-2023/

January 10-11, 2023

Software Supply Chain Assurance Home

Source: https://na.eventscloud.com/website/23612/

January 24-25, 2023

The Must Attend Event for Chip, Board, and Systems Design Engineers

Source: https://www.designcon.com/en/home.html

January 31 - February 2, 2023

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Semicon korea 2023 to showcase sustainability smart manufacturing advanced chip technologies and talent

Source: https://www.semi.org/en/news-media-press-releases/semi-press-releases/semicon-korea-2023-to-showcase-sustainability-smart-manufacturing-advanced-chip-technologies-and-talent

February 1-3, 2023

GRIMM's Defensive Automotive Engineering Security Training | GRIMM Cyber

Source: https://grimm.coursestorm.com/course/grimm-s-defensive-automotive-engineering-security-training1

February 6, 2023

Parts and Material Management Conference

Source: http://pmmcmeeting.org/

February 6-9, 2022

Cybersecurity Standardisation Conference 2023

Source: https://www.enisa.europa.eu/events/cybersecurity_standardisation_2023

February 7, 2023

The S4 SBOM Challenge

Source: https://dale-peterson.com/2022/09/06/the-s4-sbom-challenge/

February 14-16, 2023

Summary: The SBOM Challenge will test competitors in three tasks: 1. Create an accurate SBOM 2. Identify known vulnerabilities in the components in the SBOM 3.

Link back to Table of Contents

The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Read in and apply vulnerability applicability data feeds (VEX and possibly others)

Phoenix Challenge 2023

Source: https://phoenix-challenge-new.webflow.io/

February 27 - March 3, 2023

Symposium on Counterfeit Parts and Materials - United Kingdom

Source: https://smta.org/events/EventDetails.aspx?id=1665471&group=

March 14-15, 2023

13th Annual NICE Conference and Expo

Source: https://www.nist.gov/news-events/events/2023/06/13th-annual-nice-conference-and-expo

June 5-7, 2023

Request for Comments

Intent To Request an Extension From OMB of One Current Public Collection of Information: Cybersecurity Measures for Surface Modes

Source: https://www.federalregister.gov/documents/2022/11/14/2022-24621/intent-to-request-an-extension-from-omb-of-one-current-public-collection-of-information

Comments due: January 13, 2023

SP 1800-22 (Draft) - Mobile Device Security: Bring Your Own Device (BYOD) (2nd Draft)

Source: https://csrc.nist.gov/publications/detail/sp/1800-22/draft

Link back to Table of Contents

Comments due: January 13, 2023

SP 800-188 (Draft) - De-Identifying Government Data Sets (3rd Draft)

Source: https://csrc.nist.gov/publications/detail/sp/800-188/draft

Comments due: January 15, 2023

Enhancing Surface Cyber Risk Management

Source: https://www.federalregister.gov/documents/2022/11/30/2022-25941/enhancing-surface-cyber-risk-management

Comments due: January 17, 2022

Additional sources:
https://industrialcyber.co/transport/tsa-seeks-feedback-on-improving-surface-cyber-risk-management-across-transportation-systems/?

Project 2020-06 Verifications of Models and Data for Generators

Source: https://www.nerc.com:443/pa/Stand/Pages/Project-2020_06-Verifications-of-Models-and-Data-for-Generators.aspx

Comments due: January 18, 2023

National Cybersecurity Center of Excellence (NCCoE) Responding to and Recovering From a Cyberattack: Cybersecurity for the Manufacturing Sector

Source: https://www.federalregister.gov/documents/2022/12/23/2022-27995/national-cybersecurity-center-of-excellence-nccoe-responding-to-and-recovering-from-a-cyberattack

Comments due: January 23, 2023

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Additional sources:
https://content.govdelivery.com/accounts/USNIST/bulletins/33e524c

SP 1800-36 (Draft) - Trusted Internet of Things (IoT) Device Network-Layer Onboarding and Lifecycle Management: Enhancing Internet Protocol-Based IoT Device and Network Security (Preliminary Draft)

Source: https://csrc.nist.gov/publications/detail/sp/1800-36/draft

Comments due: February 3, 2023

SP 800-55 Rev. 2 (Draft), Performance Measurement Guide for Information Security

Source: https://csrc.nist.gov/publications/detail/sp/800-55/rev-2/draft

Comments due: February 13, 2023

Journal of Hardware and Systems Security

Source: https://www.springer.com/journal/41635/updates/23638886

Submission deadline: March 1, 2023

From the Article: "This special issue aims to cover all security and privacy issues in memory chips, emerging memory technologies, and in-memory computing, along with how these can be used in developing security primitives for supply chain security and cryptographic operations."

Call for Expression of Interest Cross border SOC platforms

Source: https://cybersecurity-centre.europa.eu/system/files/2022-11/Call%20for%20Expression%20of%20Interest_Cross-border%20SOC%20platformsfinal.pdf

Additional sources:
https://industrialcyber.co/news/eu-calls-upon-select-entities-in-member-states-to-host-

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

operate-cross-border-cyber-threat-detection-platforms/

NIST SP 800-63-4 (Draft), Digital Identity Guidelines

Source: https://csrc.nist.gov/publications/detail/sp/800-63/4/draft

Comments due: March 24, 2023

From the Article: "NIST requests comments on the draft fourth revision to the four-volume suite of Special Publication 800-63, Digital Identity Guidelines."

Patches/Advisories

Schneider Electric APC Easy UPS Online
https://us-cert.cisa.gov/ics/advisories/icsa-22-347-02

Mozilla Releases Security Updates for Thunderbird and Firefox
https://us-cert.cisa.gov/ncas/current-activity/2022/12/13/mozilla-releases-security-updates-thunderbird-and-firefox

VMware Releases Security Updates for Multiple products
https://us-cert.cisa.gov/ncas/current-activity/2022/12/13/vmware-releases-security-updates-multiple-products

CISA Adds Five Known Exploited Vulnerabilities to Catalog
https://us-cert.cisa.gov/ncas/current-activity/2022/12/13/cisa-adds-five-known-exploited-vulnerabilities-catalog

CISA Adds One Known Exploited Vulnerability to Catalog
https://us-cert.cisa.gov/ncas/current-activity/2022/12/14/cisa-adds-one-known-exploited-vulnerability-catalog

Siemens APOGEE/TALON Field Panels
https://us-cert.cisa.gov/ics/advisories/icsa-22-349-10

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Prosys OPC UA Simulation Server
https://us-cert.cisa.gov/ics/advisories/icsa-22-349-01

Siemens SCALANCE X-200RNA Switch Devices
https://us-cert.cisa.gov/ics/advisories/icsa-22-349-02

Siemens Multiple Denial of Service Vulnerabilities in Industrial Products
https://us-cert.cisa.gov/ics/advisories/icsa-22-349-03

Siemens Multiple Vulnerabilities in SCALANCE Products
https://us-cert.cisa.gov/ics/advisories/icsa-22-349-04

Siemens PLM Help Server
https://us-cert.cisa.gov/ics/advisories/icsa-22-346-05

Siemens SIMATIC WinCC OA Ultralight Client
https://us-cert.cisa.gov/ics/advisories/icsa-22-349-06

Siemens Simcenter STAR-CCM+
https://us-cert.cisa.gov/ics/advisories/icsa-22-349-07

Siemens Polarion ALM
https://us-cert.cisa.gov/ics/advisories/icsa-22-349-08

Siemens Products affected by OpenSSL 3.0
https://us-cert.cisa.gov/ics/advisories/icsa-22-349-09

CISA Releases Forty-One Industrial Control Systems Advisories
https://us-cert.cisa.gov/ncas/current-activity/2022/12/15/cisa-releases-forty-one-industrial-control-systems-advisories

Drupal Releases Security Updates to Address Vulnerabilities in H5P and File (Field)

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Paths
https://us-cert.cisa.gov/ncas/current-activity/2022/12/15/drupal-releases-security-updates-address-vulnerabilities-h5p-and

Review – 20 Advisories Published – 12-15-22
https://chemical-facility-security-news.blogspot.com/2022/12/review-20-advisories-published-12-15-22.html

Review – 21 Advisories Published – 12-15-22
https://chemical-facility-security-news.blogspot.com/2022/12/review-21-advisories-published-12-15-22.html

FBI, FDA OCI, and USDA Release Joint Cybersecurity Advisory Regarding Business Email Compromise Schemes Used to Steal Food
https://us-cert.cisa.gov/ncas/current-activity/2022/12/16/fbi-fda-oci-and-usda-release-joint-cybersecurity-advisory

Samba Releases Security Updates
https://us-cert.cisa.gov/ncas/current-activity/2022/12/16/samba-releases-security-updates

Denial of service in Siemens SIPROTEC 5 Devices
https://www.cybersecurity-help.cz/vdb/SB2022121629

Denial of service in Siemens SIPROTEC 5 Devices
https://www.cybersecurity-help.cz/vdb/SB2022121628

Multiple vulnerabilities in Siemens SCALANCE SC-600 Family
https://www.cybersecurity-help.cz/vdb/SB2022121626

NULL pointer dereference in OpenSSL
https://www.cybersecurity-help.cz/vdb/SB2022121623

Multiple vulnerabilities in Siemens SCALANCE X-200RNA Switch Devices

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

https://www.cybersecurity-help.cz/vdb/SB2022121621

Privilege escalation in Siemens Simcenter STAR-CCM+
https://www.cybersecurity-help.cz/vdb/SB2022121535

Host Header Injection in Siemens Polarion ALM
https://www.cybersecurity-help.cz/vdb/SB2022121534

Multiple vulnerabilities in several Siemens Products
https://www.cybersecurity-help.cz/vdb/SB2022121532

Out-of-bounds read in Siemens Teamcenter Visualization and JT2Go
https://www.cybersecurity-help.cz/vdb/SB2022121510

Multiple vulnerabilities in Siemens Teamcenter Visualization and JT2Go
https://www.cybersecurity-help.cz/vdb/SB2022121509

Review – Public ICS Disclosures – Week of 12-10-22 – Part 2
https://chemical-facility-security-news.blogspot.com/2022/12/review-public-ics-disclosures-week-of_18.html

CISA Advisory Update Numbering Error – 12-15-22
https://chemical-facility-security-news.blogspot.com/2022/12/cisa-advisory-update-numbering-error-12.html

Review – Public ICS Disclosures – Week of 12-10-22 – Part 1
https://chemical-facility-security-news.blogspot.com/2022/12/review-public-ics-disclosures-week-of_17.html

Use of a broken or risky cryptographic algorithm in Siemens SCALANCE Products
https://www.cybersecurity-help.cz/vdb/SB2022121924

Multiple vulnerabilities in Siemens SCALANCE Products

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

https://www.cybersecurity-help.cz/vdb/SB2022121925

Remote code execution in Siemens SCALANCE Products
https://www.cybersecurity-help.cz/vdb/SB2022121923

Insufficiently protected credentials in Prosys OPC UA Simulation Server
https://www.cybersecurity-help.cz/vdb/SB2022121910

Fuji Electric Tellus Lite V-Simulator
https://us-cert.cisa.gov/ics/advisories/icsa-22-354-01

Rockwell Automation GuardLogix and ControlLogix controllers
https://us-cert.cisa.gov/ics/advisories/icsa-22-354-02

ARC Informatique PcVue
https://us-cert.cisa.gov/ics/advisories/icsa-22-354-03

Rockwell Automation MicroLogix 1100 and 1400
https://us-cert.cisa.gov/ics/advisories/icsa-22-354-04

Delta 4G Router DX-3021
https://us-cert.cisa.gov/ics/advisories/icsa-22-354-05

Review – 5 Advisories and 1 Update Published – 12-20-22
https://chemical-facility-security-news.blogspot.com/2022/12/review-5-advisories-and-1-update.html

Priva TopControl Suite
https://us-cert.cisa.gov/ics/advisories/icsa-22-356-01

Mitsubishi Electric MELSEC iQ-R, iQ-L Series and MELIPC Series
https://us-cert.cisa.gov/ics/advisories/icsa-22-356-03

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Omron CX-Programmer
https://us-cert.cisa.gov/ics/advisories/icsa-22-356-04

CISA Releases Four Industrial Control Systems Advisories
https://us-cert.cisa.gov/ncas/current-activity/2022/12/22/cisa-releases-four-industrial-control-systems-advisories

Review – 4 Advisories Published – 12-22-22
https://chemical-facility-security-news.blogspot.com/2022/12/review-4-advisories-published-12-22-22.html

Review – Public ICS Disclosures – Week of 12-17-22
https://chemical-facility-security-news.blogspot.com/2022/12/review-public-ics-disclosures-week-of_24.html

Patches/Advisories Articles of Interest

Microsoft Reclassifies SPNEGO Extended Negotiation Security Vulnerability as 'Critical'

Source: https://thehackernews.com/2022/12/microsoft-reclassifies-spnego-extended.html

From the Article: "Microsoft has revised the severity of a security vulnerability it originally patched in September 2022, upgrading it to "Critical" after it emerged that it could be exploited to achieve remote code execution."

Additional sources:
https://securityintelligence.com/posts/critical-remote-code-execution-vulnerability-spnego-extended-negotiation-security-mechanism/

https://thehackernews.com/2022/12/microsoft-reclassifies-spnego-extended.html

https://www.tenable.com/blog/cve-2022-37958-faq-for-critical-microsoft-spnego-negoex-vulnerability

https://heimdalsecurity.com/blog/spnego-vulnerability-lets-attackers-execute-code-remotely/

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

December 2022 Patch Tuesday fixed 2 zero-day flaws

Source: https://securityaffairs.co/wordpress/139640/security/december-2022-patch-tuesday.html

From the Article: "Six vulnerabilities are rated Critical, 43 Important, and three are Moderate in severity. Microsoft December 2022 Patch Tuesday security updates fixed two zero-day vulnerabilities; one of the new issues addressed this month is listed as publicly known at the time of release, and one is actively exploited."

Microsoft Details Recent macOS Gatekeeper Bypass Vulnerability

Source: https://www.securityweek.com/microsoft-details-recent-macos-gatekeeper-bypass-vulnerability

From the Article: "Microsoft this week shared details on CVE-2022-42821, a Gatekeeper bypass vulnerability that Apple recently addressed in macOS Ventura, Monterey, and Big Sur."

FoxIt Patches Code Execution Flaws in PDF Tools

Source: https://www.securityweek.com/foxit-patches-code-execution-flaws-pdf-tools

From the Article: "Foxit Software has rolled out a critical-severity patch to cover a dangerous remote code execution flaw in its flagship PDF Reader and PDF Editor products."

Old vulnerabilities in Cisco products actively exploited in the wild

Source: https://securityaffairs.co/wordpress/139821/security/cisco-old-vulnerabilities-exploitation.html

From the Article: "Cisco has updated multiple security advisories to warn of the active exploitation of several old vulnerabilities impacting its products."

CISA adds Veeam Backup and Replication bugs to Known Exploited Vulnerabilities Catalog

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Source: https://securityaffairs.co/wordpress/139731/hacking/veeam-backup-known-exploited-vulnerabilities-catalog.html

From the Article: "US CISA added two vulnerabilities impacting Veeam Backup & Replication software to its Known Exploited Vulnerabilities Catalog."

Apple fixed the tenth actively exploited zero-day this year

Source: https://securityaffairs.co/wordpress/139635/hacking/apple-tenth-actively-exploited-zero-day.html

From the Article: "Apple rolled out security updates to iOS, iPadOS, macOS, tvOS, and Safari to fix a new actively exploited zero-day (CVE-2022-42856)."

Critical Microsoft Code-Execution Vulnerability

Source: https://www.schneier.com/blog/archives/2022/12/critical-microsoft-code-execution-vulnerability.html

From the Article: "A critical code-execution vulnerability in Microsoft Windows was patched in September."

New Microsoft Exchange exploit chain lets ransomware attackers in (CVE-2022-41080)

Source: https://www.helpnetsecurity.com/2022/12/21/cve-2022-41080/

From the Article: "Ransomware-wielding attackers are using a new exploit chain that includes one of the ProxyNotShell vulnerabilities (CVE-2022-41082) to achieve remote code execution on Microsoft Exchange servers."

Microsoft Fixes Two Zero-Day Vulnerabilities on December Patch Tuesday

Source: https://www.cysecurity.news/2022/12/microsoft-fixes-two-zero-day.html

From the Article: "Microsoft has patched 48 new flaws in its products, including one that attackers are currently employing as well as one that has been made public but is not currently being actively used by attackers. "

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

CISA Warns Veeam Backup & Replication Vulnerabilities Exploited in Attacks

Source: https://www.securityweek.com/cisa-warns-veeam-backup-replication-vulnerabilities-exploited-attacks

From the Article: "The US Cybersecurity and Infrastructure Security Agency (CISA) has added two flaws affecting Veeam's Backup & Replication product to its Known Exploited Vulnerabilities Catalog."

SAP's December 2022 Security Updates Patch Critical Vulnerabilities

Source: https://www.securityweek.com/saps-december-2022-security-updates-patch-critical-vulnerabilities

From the Article: "German software maker SAP this week announced the release of 14 new and five updated security notes as part of its December 2022 Security Patch Day, including four notes that address critical vulnerabilities in Business Client, BusinessObjects, NetWeaver, and Commerce."

High-Severity Memory Safety Bugs Patched With Latest Chrome 108 Update

Source: https://www.securityweek.com/high-severity-memory-safety-bugs-patched-latest-chrome-108-update

From the Article: "Google this week announced a Chrome update that resolves eight vulnerabilities in the popular browser, including five reported by external researchers."

Apple Patches Zero-Day Vulnerability Exploited Against iPhones

Source: https://www.securityweek.com/apple-patches-zero-day-vulnerability-exploited-against-iphones

From the Article: "Apple on Tuesday published 10 new advisories describing vulnerabilities affecting its products, including a zero-day that has been exploited against iPhone users."

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Adobe Patches 38 Flaws in Enterprise Software Products

Source: https://www.securityweek.com/adobe-patches-38-flaws-enterprise-software-products

From the Article: "After skipping last month, Adobe returned to its scheduled Patch Tuesday cadence with the release of fixes for at least 38 vulnerabilities in multiple enterprise-facing products."

CVE-2022-42475: Fortinet Pre-authentication Code-execution Vulnerability

Source: https://www.recordedfuture.com/cve-2022-42475-fortinet-pre-authentication-code-execution-vuln

From the Article: "Fortinet continues to garner and release information to address a recently-discovered heap-based buffer overflow vulnerability impacting several versions of FortiOS (FOS), the operating system behind an entire series of FortiGate next-generation firewalls and security appliances."

Patch Tuesday: Microsoft Plugs Windows Hole Exploited in Ransomware Attacks

Source: https://www.securityweek.com/patch-tuesday-microsoft-plugs-windows-hole-exploited-ransomware-attacks

From the Article: "The operating system update, released as part of Microsoft's scheduled Patch Tuesday, addresses a flaw that lets malicious attackers use rigged files to evade MOTW (Mart of the Web) defenses."

Microsoft patches Windows zero-day used to drop ransomware - Bleeping Computer

Source: https://www.bleepingcomputer.com/news/security/microsoft-patches-windows-zero-day-used-to-drop-ransomware/

From the Article: "Microsoft has fixed a security vulnerability used by threat actors to circumvent the Windows SmartScreen security feature and deliver payloads in Magniber ransomware attacks."

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Microsoft Patches Zero-Day Magniber Ransomware Hackers Used - BankInfoSecurity

Source: https://www.bankinfosecurity.com/microsoft-patches-0day-used-by-magniber-ransomware-attackers-a-20711

From the Article: "A fix for a zero-day vulnerability exploited by ransomware hackers is part of this month's patch dump from operating system Microsoft."

Heap-based buffer overflow vulnerability in Fortinet FortiOS SSL-VPN appliances, patches available

Source: https://industrialcyber.co/vulnerabilities/heap-based-buffer-overflow-vulnerability-in-fortinet-fortios-ssl-vpn-appliances-patches-available/

From the Article: "Fortinet announced Monday that the presence of a heap-based buffer overflow vulnerability [CWE-122] in FortiOS SSL-VPN may allow a remote unauthenticated attacker to execute arbitrary code or commands via specifically crafted requests."

Apple Fixes Actively Exploited iPhone Zero-Day Vulnerability

Source: https://www.infosecurity-magazine.com/news/apple-fixes-exploited-iphone-zero/

From the Article: "The vulnerability could allow remote code execution (RCE) on a victim's device."

The December 2022 Patch Tuesday Security Update Review

Source: https://blog.qualys.com/vulnerabilities-threat-research/patch-tuesday/2022/12/13/the-december-2022-patch-tuesday-security-update-review

From the Article: "Welcome to the final second Tuesday of the year. As expected, Microsoft and Adobe have released their latest security updates and fixes. Take a break from your holiday preparations and join us as we review the details of the latest security patches. "

Link back to Table of Contents

CVE-2022-28703

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-28703

From the Article: "A stored cross-site scripting vulnerability exists in the HdConfigActions.aspx altertextlanguages functionality of Lansweeper lansweeper 10.1.1.0. A specially-crafted HTTP request can lead to arbitrary Javascript code injection."

Windows Zero-day Exploited for Ransomware Was Fixed

Source: https://heimdalsecurity.com/blog/windows-zero-day-exploited-ransomware-fixed/

From the Article: "Microsoft announced an important zero-day that threat actors used for launching ransomware attacks was resolved during the latest Patch Tuesday. The team has been working to find a solution since October."

Citrix ADC and Gateway Zero Day Exploited by Hackers

Source: https://heimdalsecurity.com/blog/citrix-adc-and-gateway-zero-day-exploited-by-hackers/

From the Article: "Citrix urgently advises administrators to install security updates for Citrix ADC and Gateway due to a “Critical” zero-day vulnerability (CVE-2022-27518) that is being actively exploited by state-sponsored hackers to access business networks."

New Actively Exploited Zero-Day Vulnerability Discovered in Apple Products

Source: https://heimdalsecurity.com/blog/new-actively-exploited-zero-day-vulnerability-discovered-in-apple-products/

From the Article: "Earlier this week, Apple released updates to reinforce their security against a new zero-day vulnerability that could lead to the execution of malicious code. Old CVE-2022-42856 is a type of confusion issue within the WebKit browser engine."

Link back to Table of Contents

Patch Tuesday December 2022 – Microsoft Fixes Spoofing and Elevation of Privilege Vulnerabilities

Source: https://heimdalsecurity.com/blog/patch-tuesday-december-2022/

From the Article: "The end of the year is here, and with it, Microsoft is trying to wrap up some loose ends with their Edge browser for the final Patch Tuesday of 2022."

Critical FortiOS pre-auth RCE vulnerability exploited by attackers (CVE-2022-42475)

Source: https://www.helpnetsecurity.com/2022/12/13/cve-2022-42475/

From the Article: "A critical RCE vulnerability (CVE-2022-42475) in Fortinet's operating system, FortiOS, is being exploited by attackers, reportedly by a ransomware group. "Fortinet is aware of an instance where this vulnerability was exploited in the wild," the company said in an advisory published on Monday, but offered no specific details about the attack."

State-sponsored attackers actively exploiting RCE in Citrix devices, patch ASAP! (CVE-2022-27518)

Source: https://www.helpnetsecurity.com/2022/12/13/cve-2022-27518-exploited/

From the Article: "An unauthenticated remote code execution flaw (CVE-2022-27518) is being leveraged by a Chinese state-sponsored group to compromise Citrix Application Delivery Controller (ADC) deployments, the US National Security Agency has warned."

Apple Zero-Day Actively Exploited on iPhone 15

Source: https://www.darkreading.com/attacks-breaches/apple-zero-day-actively-exploited-iphone-15

From the Article: "Without many details, Apple patches a vulnerability that has been exploited in the wild to execute code."

Microsoft Squashes Zero-Day, Actively Exploited Bugs in Dec. Update

Source: https://www.darkreading.com/application-security/microsoft-squashes-zero-day-

Link back to Table of Contents

The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

actively-exploited-bugs-dec-update

From the Article: "Here's what you need to patch now, including six critical updates for Microsoft's final Patch Tuesday of the year."

Critical Patches Issued for Microsoft Products

Source: https://www.cisecurity.org/advisory/critical-patches-issued-for-microsoft-products_2022-146

From the Article: "Multiple vulnerabilities have been discovered in Microsoft products, the most severe of which could allow for remote code execution in the context of the logged on user."

Microsoft Patch Tuesday for December 2022 — Snort rules and prominent vulnerabilities

Source: https://blog.talosintelligence.com/microsoft-patch-tuesday-for-december-2022/

From the Article: "Microsoft released its monthly security update on Tuesday, disclosing 48 vulnerabilities. Of these vulnerabilities, 6 are classified as “Critical”, 41 are classified as “Important”, with the remaining vulnerability classified as “Moderate.”"

December 2022 Patch Tuesday: 10 Critical CVEs, One Zero-Day, One Under Active Attack

Source: http://provinggrounds.cs.sys/blog/patch-tuesday-analysis-december-2022/

From the Article: "Microsoft has released 49 security patches for its December 2022 Patch Tuesday rollout. Of these, 10 vulnerabilities are rated Critical, two are rated Medium and the rest are rated Important. DirectX Graphics Kernel Elevation of Privilege Vulnerability (CVE-2022-44710) is listed as publicly known while Windows SmartScreen Security Feature Bypass Vulnerability (CVE-2022-44698) is listed as actively exploited at the time of release."

December 2022 Patch Tuesday: Get Latest Security Updates from Microsoft and More

Source: https://thehackernews.com/2022/12/december-2022-patch-tuesday-get-latest.html

Link back to Table of Contents

From the Article: "Tech giant Microsoft released its last set of monthly security updates for 2022 with fixes for 49 vulnerabilities across its software products."

CVE-2022-42475: Fortinet Patches Zero Day in FortiOS SSL VPNs

Source: https://www.tenable.com/blog/cve-2022-42475-fortinet-patches-zero-day-in-fortios-ssl-vpns

From the Article: "Fortinet has patched a zero day buffer overflow in FortiOS that could lead to remote code execution. There has been a report of active exploitation and organizations should patch urgently."

Podcasts/Videos

How To Get Started in Information Security - PSW #767

Source: https://www.youtube.com/watch?v=GCOxSwX7TAo

Chinese-made drones spotted over DC raise national security, spying concerns | Fox News Video

Source: https://www.foxnews.com/video/6316075534112

The Defense Standardization Program

Source: https://www.youtube.com/watch?v=msB_1AOmPGA

WATCH: Intel Federal's Steve Orrin on Supply Chain Resiliency, Cyber Risk Management - WashingtonExec

Source: https://washingtonexec.com/2022/12/watch-intel-federals-steve-orrin-on-supply-chain-resiliency-and-cyber-risk-management/

U.S. Department of Commerce Roundtable for U.S. and European Stakeholders

Source: https://www.youtube.com/watch?v=MHH6TmAwlEo

Link back to Table of Contents

The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Survey: Tech executives say cloud computing and security are top priority

Source: https://www.cnbc.com/video/2022/12/19/survey-tech-executives-say-cloud-computing-and-security-are-top-priority.html

PCII Program Introduction Video

Source: https://www.youtube.com/watch?v=KHJR8lS5Zto

The History of the FPGA: The Ultimate Flex

Source: https://www.youtube.com/watch?v=m-8G1Yixb34

Watch CBS Evening News: TikTok faces growing national security concerns - Full show on CBS

Source: https://www.cbs.com/shows/video/oZlQQoySEVUEYpfbUSKdwPnZEnXZVpZH/

The Business & Legal Risks of not Complying with DFARS 7012 & CMMC

Source: https://www.youtube.com/watch?v=ku8ELKYrAHw

Chip outlook: Auto sector the 'leading revenue driver for 2023,' analyst says

Source: https://finance.yahoo.com/video/chip-outlook-auto-sector-leading-153751302.html

Adam Meyers from CrowdStrike head of threat intelligence discusses Nation-state-sponsored activity through diplomatic, political, military and economic espionage as well as describing disruptive offensive cyber operations.

Source: https://thecyberwire.com/podcasts/interview-selects/140/notes

Link back to Table of Contents

The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

From the Article: "This interview from December 23rd, 2022 originally aired as a shortened version on the CyberWire Daily Podcast."

PolyVice and Royal ransomware make nuisances of themselves. US warns that KillNet can be expected to go after the healthcare sector. CISA's plans for stakeholder engagement.

Source: https://thecyberwire.com/podcasts/daily-podcast/1730/notes

From the Article: "The Vice Society may be upping its marketing game. Royal ransomware may have a connection to Conti. Royal delivers ransom note by hacked printer. KillNet goes after healthcare."

Developing a banking Trojan into a newer, more effective form. Cyberattacks on media outlets. Abuse of AWS Elastic IP transfer. Notes on the hybrid war. And cybercrooks are inspired by Breaking Bad.

Source: https://thecyberwire.com/podcasts/daily-podcast/1728/notes

From the Article: "The Godfather banking Trojan has deep roots in older code. FuboTV was disrupted around its World Cup coverage. The Guardian has been hit with an apparent ransomware attack."

Warnings on SentinelSneak. The rise of malicious XLLs. Updates from Russia's hybrid war. An unusually loathsome campaign targets children.

Source: https://thecyberwire.com/podcasts/daily-podcast/1727/notes

From the Article: "SentinelSneak is out in the wild. XLLs for malw are delivery. CERT-UA warns of attacks against the DELTA situational awareness system. FSB cyber operations against Ukraine. "

Malicious apps do more than extort predatory loans. A Facebook account recovery scam. Notes from the hybrid war. Goodbye SHA-1, hello Leviathans.

Source: https://thecyberwire.com/podcasts/daily-podcast/1725/notes

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

From the Article: "A predatory loan app is discovered embedded in mobile apps. Facebook phishing. GPS disruptions are reported in Russian cities. NSA warns against dismissing Russian offensive cyber capabilities."

BEC gets into bulk food theft. BlackCat ransomware update. Epic Games' settlement with FTC. InfraGard data taken down. More on the hybrid war. And Twitter asks for the voice of the people.

Source: https://thecyberwire.com/podcasts/daily-podcast/1726/notes

From the Article: "BEC takes aim at physical goods (including food). BlackCat ransomware activity increases. Epic Games settles an FTC regulatory case. The InfraGard database was pulled from a dark web auction site."

The Core of the Problem With OT Control System Security - BankInfoSecurity.com

Source: https://www.bankinfosecurity.com/interviews/isolating-control-systems-i-5198

Summary: PODCAST: Joe Weiss is featured on a podcast talking about OT Control System Security, specifically Modbus Serial. Commonly used as a sensor protocol.

Regulations

CISA PUBLISHES TECHNICAL RULE TO UPDATE PROTECTED CRITICAL INFRASTRUCTURE INFORMATION (PCII) PROGRAM

Source: https://www.cisa.gov/blog/2022/12/21/cisa-publishes-technical-rule-update-protected-critical-infrastructure-information

From the Article: "WASHINGTON—Today, the Department of Homeland Security (DHS) and Cybersecurity and Infrastructure Security Agency (CISA) are issuing a technical rule to improve and modernize aspects of the Protected Critical Infrastructure Information (PCII) Program, which provides legal protections for cyber and physical infrastructure information submitted to DHS."

Additional sources:
https://industrialcyber.co/regulation-standards-and-compliance/dhs-cisa-roll-out-technical-rule-to-update-pcii-program-bring-legal-protections-for-cyber-physical-infrastructure-information/

Link back to Table of Contents

The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Reports - Government

Ctr DOD MICROELECTRONICS FPGA OVERALL ASSURANCE PROCESS PDF

Source: https://media.defense.gov/2022/Dec/08/2003127937/-1/-1/0/CTR_DOD_MICROELECTRONICS-FPGA_OVERALL_ASSURANCE_PROCESS.PDF

Ctr DOD MICROELECTRONICS FPGA BEST PRACTICES THREAT CATALOG PDF

Source: https://media.defense.gov/2022/Dec/08/2003127935/-1/-1/0/CTR_DOD_MICROELECTRONICS-FPGA_BEST_PRACTICES_THREAT_CATALOG.PDF

Ctr DOD MICROELECTRONICS FPGA LOA1 BEST PRACTICES PDF

Source: https://media.defense.gov/2022/Dec/08/2003127936/-1/-1/0/CTR_DOD_MICROELECTRONICS-FPGA_LOA1_BEST_PRACTICES.PDF

Ctr DOD MICROELECTRONICS THIRD PARTY IP REVIEW PROCESS FOR LOA1 PDF

Source: https://media.defense.gov/2022/Dec/08/2003127959/-1/-1/0/CTR_DOD_MICROELECTRONICS-THIRD_PARTY_IP_REVIEW_PROCESS_FOR_LOA1.PDF

Cyber Europe 2022: After Action Report

Source: https://www.enisa.europa.eu/publications/cyber-europe-2022-after-action-report

Cyber Criminals Impersonating Brands Using Search Engine Advertisement Services to Defraud Users

Source: https://www.ic3.gov/Media/Y2022/PSA221221

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

NSA report focuses on driving cybersecurity outcomes while pushing strong partnerships and education

Source: https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3247606/nsa-publishes-2022-cybersecurity-year-in-review/

Summary: NSA has released their Cybersecurity year in review for 2022, highlighting collaboration, threats, and industry focus over the past year.

Link to report: https://media.defense.gov/2022/Dec/15/2003133594/-1/-1/0/0139_CSD_YIR22_FINAL_LOWSIDE_ACCESSIBLE_FINAL_V2.PDF

Additional sources:
https://industrialcyber.co/reports/nsa-report-focuses-on-driving-cybersecurity-outcomes-while-pushing-strong-partnerships-and-education/

Reports - Industry

Orange Cyberdefense: Security Navigator 2023

Source: https://www.orangecyberdefense.com/global/security-navigator

Securing the Microelectronics Supply Chain

Source: https://www.rand.org/pubs/perspectives/PEA1394-1.html

In this Comphrensive Report, You'll Discover:

Source: https://info.cybersheath.com/Download-Defenseless-The-State-of-the-DIB-Merrill-Research

Supervision of financial market infrastructures annual report 2022 pdf

Source: https://www.bankofengland.co.uk/-/media/boe/files/annual-report/2022/supervision-of-financial-market-infrastructures-annual-report-

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

2022.pdf?la=en&hash=15CFDFF14FB4C1D181CF53F7EB8F9815D9DB9845

In Focus: The Two Main Drivers of Cyber Loss - Cyber Risk Insight Index - Q4 2022

Source: https://insights.corvusinsurance.com/cyber-risk-insight-index-q4-2022/in-focus-the-two-main-drivers-of-cyber-loss

State cio top ten policy and technology priorities for 2022

Source: https://www.nascio.org/resource-center/resources/state-cio-top-ten-policy-and-technology-priorities-for-2022/

The near and far future of ransomware

Source: https://documents.trendmicro.com/assets/white_papers/wp-the-near-and-far-future-of-ransomware.pdf

The convergence of IT and OT | Security Insider

Source: https://www.microsoft.com/en-us/security/business/security-insider/cyber-signals-1/the-convergence-of-it-and-ot/

Axio 2022 Ransomware Preparedness Report

Source: https://learn.axio.com/ransomware22

2023 Global Digital Trust Insights Survey

Source: https://www.pwc.com/gx/en/issues/cybersecurity/global-digital-trust-insights.html

Annual Malicious Risk Report
Source: https://www.chcglobal.co.uk/resources/

Link back to Table of Contents

The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Cyber Resilient Weapon System - Body of Knowledge
Source: https://www.crws-bok.org/

NERC Security Integration Strategy set to integrate cyber and physical security into grid planning, design, operation - Industrial Cyber
Source: https://industrialcyber.co/utilities-energy-power-water-waste/nerc-security-integration-strategy-set-to-integrate-cyber-and-physical-security-into-grid-planning-design-operation/

From the Article: "The North American Electric Reliability Corporation (NERC) announced its Security Integration Strategy that is focused on risk identification and validation, prioritization, and development of possible mitigations. It further outlines electric reliability organization (ERO) priorities to enhance security integration through working collaboratively with electricity sector stakeholders. "

Nerc Security Integration Strategy 2022 pdf
Source:
https://www.nerc.com/comm/Documents/NERC_Security_Integration_Strategy_2022.pdf

Its not a data breach its a surprise backup pdf
Source: https://liberalforum.eu/wp-content/uploads/2022/12/Its-not-a-data-breach-its-a-surprise-backup.pdf

Cyber security considerations 2022 pdf
Source: https://assets.kpmg/content/dam/kpmg/xx/pdf/2021/11/cyber-security-considerations-2022.pdf

Infusing Advanced Manufacturing into Undergraduate Engineering Education

Source: https://nap.nationalacademies.org/catalog/26773/infusing-advanced-manufacturing-into-undergraduate-engineering-education

EXCLUSIVE: Pentagon not prepared for software updates at the speed of war, report finds

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Source: https://breakingdefense.com/2022/12/exclusive-pentagon-not-prepared-for-software-updates-at-the-speed-of-war-report-finds/

Summary: A report released by Hudson Institute identifies that the Pentagon is not prepared to handle software updates on fighting systems during war time operations. The authors identify the issue and advise on techniques that can help mitigate getting software updates to fielded systems.

Link to Hudson Institute report: https://www.hudson.org/technology/software-defines-tactics

2022 NERC Long Term Reliability Assessment Release

Source: https://www.nerc.com/news/Headlines%20DL/2022_LTRA_Release.pdf

Summary: From the announcement today: “The bulk power system is undergoing unprecedented change on a scale and at a speed that challenges the ability to foresee and design for its future state,” said John Moura, NERC’s director of Reliability Assessment and Performance Analysis."

Link to report: https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC_LTRA_2022.pdf

New Agenda Ransomware Variant, Written in Rust, Aiming at Critical Infrastructure

Source: https://thehackernews.com/2022/12/new-agenda-ransomware-variant-written.html

Summary: HackerNews summarizes findings from TrendMicro on a Rust-based Agenda ransomware variant. This variant is aiming for new industries, including critical infrastructure

Link to TrendMicro report: https://www.trendmicro.com/en_us/research/22/l/agenda-ransomware-uses-rust-to-target-more-vital-industries.html

Trojaned Windows Installer Targets Ukraine

Source: https://www.schneier.com/blog/archives/2022/12/trojaned-windows-installer-

Link back to Table of Contents

The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

targets-ukraine.html

Summary: trojanized Windows 10 installers are being targeted to Ukraine government users.

Link to Mandiant report: https://www.mandiant.com/resources/blog/trojanized-windows-installers-ukrainian-government

Critical Microsoft Code-Execution Vulnerability

Source: https://www.schneier.com/blog/archives/2022/12/critical-microsoft-code-execution-vulnerability.html

Summary: Originally dismissed as an information disclosure vulnerability, it was determined this new CVE impacts a much broader range of devices and protocols.

Link to arstechnica article: https://arstechnica.com/information-technology/2022/12/critical-windows-code-execution-vulnerability-went-undetected-until-now/

DOE lab study details cyber risks for EVs

Source: https://www.mdpi.com/1996-1073/15/11/3931

Summary: Report on EV charging infrastructure vulnerabilities

Legislation

US Senate clears bipartisan bill that boosts national security by preparing for quantum cybersecurity risks - Industrial Cyber

Source: https://industrialcyber.co/vulnerabilities/us-senate-clears-bipartisan-bill-that-boosts-national-security-by-preparing-for-quantum-cybersecurity-risks/

From the Article: "The U.S. Senate recently passed a bipartisan legislative bill that works on strengthening national security by preparing the federal government's defenses against quantum computing-enabled data breaches."

Link back to Table of Contents

H.R.7535 - Quantum Computing Cybersecurity Preparedness Act

Source: https://www.congress.gov/bill/117th-congress/house-bill/7535/text

White House

Biden-Harris Administration Releases Inflation Reduction Act Guidebook for Clean Energy and Climate Programs | The White House

Source: https://www.whitehouse.gov/briefing-room/statements-releases/2022/12/15/biden-harris-administration-releases-inflation-reduction-act-guidebook-for-clean-energy-and-climate-programs/

Statement by National Security Advisor Jake Sullivan on Japan's Historic National Security Strategy | The White House

Source: https://www.whitehouse.gov/briefing-room/statements-releases/2022/12/16/statement-by-national-security-advisor-jake-sullivan-on-japans-historic-national-security-strategy/

Remarks by President Biden at the U.S.-Africa Leaders Summit Closing Session on Promoting Food Security and Food Systems Resilience | The White House

Source: https://www.whitehouse.gov/briefing-room/speeches-remarks/2022/12/15/remarks-by-president-biden-at-the-u-s-africa-leaders-summit-closing-session-on-promoting-food-security-and-food-systems-resilience/

U.S.-Africa Leaders Summit: Joint Statement on Food Security | The White House

Source: https://www.whitehouse.gov/briefing-room/statements-releases/2022/12/15/u-s-africa-leaders-summit-joint-statement-on-food-security/

FACT SHEET: New Initiative on Digital Transformation with Africa (DTA) | The White House
Source: https://www.whitehouse.gov/briefing-room/statements-releases/2022/12/14/fact-sheet-new-initiative-on-digital-transformation-with-africa-dta/

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Articles of Interest

The Guardian hit by suspected ransomware attack - Engadget

Source: https://www.engadget.com/the-guardian-suspected-ransomware-attack-191542719.html

From the Article: "Prominent news organizations are high-value targets for hackers and it appears that The Guardian is the latest to have fallen victim to an attack. A "serious IT incident" struck the publication on Tuesday evening."

Additional sources:
https://www.scmagazine.com/brief/ransomware/suspected-ransomware-attack-hits-guardian-newspaper

https://www.malwarebytes.com/blog/news/2022/12/the-guardian-hit-by-ransomware-attack

https://www.bbc.com/news/technology-64056300

https://www.infosecurity-magazine.com/news/ransomware-attack-guardian/

https://techcrunch.com/2022/12/21/the-guardian-ransomware/

https://www.theregister.com/2022/12/21/the_guardian_hit_by_ransomware/

https://www.bbc.com/news/technology-64056300

https://www.businesstoday.in/technology/story/british-newspaper-the-guardian-hit-by-a-ransomware-attack-357342-2022-12-22

https://www.pgurus.com/the-guardian-confirms-their-systems-were-hit-by-ransomware-attack/

https://www.infosecurity-magazine.com/news/ransomware-attack-guardian/

https://www.techcentral.ie/the-guardian-newspaper-believes-ongoing-it-incident-caused-by-ransomware/

https://www.siliconrepublic.com/enterprise/guardian-ransomware-attack-okta

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

https://www.oodaloop.com/briefs/2022/12/22/ransomware-attack-hits-the-guardian-newspaper/

https://www.cysecurity.news/2022/12/the-guardian-apparently-hit-by.html

https://www.mediapost.com/publications/article/380927/the-guardian-suffers-apparent-ransomware-attack.html

https://www.computing.co.uk/news/4061997/guardian-employees-home-suspected-ransomware-attack

https://www.theguardian.com/media/2022/dec/21/guardian-hit-by-serious-it-incident-believed-to-be-ransomware-attack

https://siliconangle.com/2022/12/21/guardian-newspaper-hacked-suspected-ransomware-attack/

https://www.telegraph.co.uk/business/2022/12/21/guardian-staff-shut-office-newspaper-suffers-glitch/

https://www.bankinfosecurity.com/guardian-ransomware-attack-may-presage-holiday-blitzkrieg-a-20769

https://www.silicon.co.uk/security/cyberwar/guardian-newspaper-ransomware-attack-491088

https://www.oodaloop.com/briefs/2022/12/22/ransomware-attack-hits-the-guardian-newspaper/

https://www.cysecurity.news/2022/12/the-guardian-apparently-hit-by.html

https://www.editorandpublisher.com/stories/british-newspaper-the-guardian-says-its-been-hit-by-ransomware,241478

https://www.securityweek.com/ransomware-attack-causes-disruption-british-newspaper-guardian

https://infotechlead.com/security/guardian-faces-ransomware-attack-on-it-systems-76037

https://www.thedailybeast.com/the-guardians-servers-hit-by-suspected-ransomware-attack

Link back to Table of Contents

The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

https://www.cybersecurityconnect.com.au/commercial/8535-the-guardian-hit-by-possible-ransomware-attack

https://www.arabnews.com/node/2220456/media

https://www.moneycontrol.com/news/technology/uks-guardian-hit-by-suspected-ransomware-attack-9746591.html

https://heimdalsecurity.com/blog/british-newspaper-the-guardian-targeted-by-cyberattack/

https://www.hackread.com/guardian-ransomware-attack/

https://techcrunch.com/2022/12/21/the-guardian-ransomware/

https://thewestnews.com/a-ransomware-attack-has-hit-the-leading-uk-based-newspaper-the-guardian/

Ransomware gang caught using Microsoft-approved drivers to hack targets - TechCrunch

Source: https://techcrunch.com/2022/12/13/cuba-ransomware-microsoft-drivers/

From the Article: "Security researchers say they have evidence that threat actors affiliated with the Cuba ransomware gang used malicious hardware drivers certified by Microsoft during an recent attempted ransomware attack."

Additional sources:
https://www.techradar.com/news/hardware-drivers-approved-by-microsoft-used-in-ransomware-attacks

https://www.scmagazine.com/news/ransomware/microsoft-blocks-threat-actors-that-obtained-signed-drivers-to-deploy-ransomware

https://www.zdnet.com/article/these-hackers-used-microsoft-signed-malicious-drivers-to-further-their-ransomware-attacks/

https://www.infosecurity-magazine.com/news/microsoft-drivers-used-in-cyber/

https://heimdalsecurity.com/blog/malicious-windows-drivers-ransomware-attacks/

https://www.hackread.com/microsoft-signed-drivers-hackers-breach/

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

https://www.bitdefender.com/blog/hotforsecurity/microsoft-approved-and-digitally-signed-malicious-drivers-used-in-ransomware-attacks/

https://www.darkreading.com/attacks-breaches/microsoft-signed-malicious-drivers-edr-killers-ransomware

https://www.csoonline.com/article/3683288/cuba-ransomware-group-used-microsoft-developer-accounts-to-sign-malicious-drivers.html

https://www.theregister.com/2022/12/14/microsoft_drivers_ransomware_attacks/

https://www.cysecurity.news/2022/12/cuban-ransomware-gang-hacked-devices.html

https://thehackernews.com/2022/12/ransomware-attackers-use-microsoft.html

https://www.helpnetsecurity.com/2022/12/13/cve-2022-44698/

https://www.bleepingcomputer.com/news/microsoft/microsoft-signed-malicious-windows-drivers-used-in-ransomware-attacks/

LastPass: Hackers Stole Customers' Password Vaults, Breach Worse Than Initially Thought

Source: https://www.cysecurity.news/2022/12/lastpass-hackers-stole-customers.html

From the Article: "This past August witnessed a breach at LastPass, one of the most well-known password manager services available. The harm caused by the unidentified hackers is significantly worse than was initially believed, according to the company. Passwords should be changed immediately by users."

Additional sources:
https://thehackernews.com/2022/12/lastpass-admits-to-severe-data-breach.html

https://www.securityweek.com/lastpass-says-password-vault-data-stolen-data-breach

https://securityaffairs.co/wordpress/139935/data-breach/lastpass-encrypted-password-vaults-stolen.html

https://thecyberwire.com/newsletters/privacy-briefing/4/245

https://www.itworldcanada.com/article/lastpass-hacker-got-customer-information-and-

Link back to Table of Contents

their-encrypted-vault-data/519601

https://www.theverge.com/2022/12/22/23523322/lastpass-data-breach-cloud-encrypted-password-vault-hackers

https://thehackernews.com/2022/12/lastpass-admits-to-severe-data-breach.html

https://www.helpnetsecurity.com/2022/12/23/lastpass-breach-customer-vault/

https://heimdalsecurity.com/blog/threat-actors-hacked-lastpass-cloud-storage-and-stole-customers-data/

https://www.hackread.com/lastpass-encrypted-password-vaults-stolen/

https://www.darkreading.com/attacks-breaches/lastpass-massive-breach-including-customer-vault-data

FBI Info Sharing Platform InfraGard Was Hacked

Source: https://heimdalsecurity.com/blog/fbi-info-sharing-platform-infragard-was-hacked/

From the Article: "Last week, a database containing the contact information of more than 80,000 InfraGard members was put up for sale. InfraGard is a project established by the Federal Bureau of Investigation (FBI) to establish partnerships with the private sector in order to share information about cyber and physical threats."

Additional sources:
https://www.darkreading.com/attacks-breaches/stolen-data-on-80k-members-of-fbi-run-infragard-reportedly-for-sale-on-dark-web-forum

https://www.cysecurity.news/2022/12/attacker-uses-infragard-devices-to.html

https://research.checkpoint.com/2022/19th-december-threat-intelligence-report/

https://krebsonsecurity.com/2022/12/fbis-vetted-info-sharing-network-infragard-hacked/

https://www.hackread.com/fbi-infragard-hacked-data-sold/

https://www.cysecurity.news/2022/12/hacking-of-us-infragard-critical.html

https://www.malwarebytes.com/blog/news/2022/12/infragard-infiltrated-by-cybercriminal

Link back to Table of Contents

https://www.securityweek.com/hacker-claims-breach-fbis-critical-infrastructure-portal

https://gizmodo.com/fbi-infragard-cybersecurity-hack-critical-infrastructur-1849893073

FBI seized 48 domains linked to DDoS-for-Hire service platforms

Source: https://securityaffairs.co/wordpress/139670/cyber-crime/fbi-ddos-for-hire-service-platforms.html

From the Article: "The U.S. Department of Justice (DoJ) this week announced the seizure of 48 domains associated with the DDoS-for-Hire Service platforms (aka Booter services) used by threat actors."

Additional sources:
https://krebsonsecurity.com/2022/12/six-charged-in-mass-takedown-of-ddos-for-hire-sites/

https://heimdalsecurity.com/blog/the-fbi-just-seized-48-domain-names-linked-to-ddos-for-hire-platforms/

https://thehackernews.com/2022/12/fbi-charges-6-seizes-48-domains-linked.html

https://www.tripwire.com/state-of-security/operation-power-50-ddos-services-taken-offline-international-crackdown

https://www.securityweek.com/us-charges-six-operation-targeting-48-ddos-hire-websites

https://www.hackread.com/fbi-ddos-hiring-services-busted/

https://www.justice.gov/usao-cdca/pr/federal-prosecutors-los-angeles-and-alaska-charge-6-defendants-operating-websites

https://www.infosecurity-magazine.com/news/feds-hit-ddosforhire-48-domain/

Hackers Claims to Have California Department of Finance Data - Government Technology

Source: https://www.govtech.com/security/hackers-claims-to-have-california-department-of-finance-data

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

From the Article: " California officials are investigating a cybersecurity incident at the Department of Finance after a global ransomware group claimed it stole confidential data and financial documents from the agency."

Additional sources:
https://www.infosecurity-magazine.com/news/california-hit-by-alledged-lockbit/

https://www.itechpost.com/articles/115544/20221214/department-finance-california-suffer-lockbit-ransomware-cyberattack.htm

https://www.technewsday.com/2022/12/14/lockbit-behind-the-ransomware-attack-on-the-california-department-of-finance/

https://heimdalsecurity.com/blog/california-state-finance-department-lockbit-ransomwares-latest-victim/

https://www.cyberscoop.com/lockbit-ransomware-california-department-of-finance/

https://www.theregister.com/2022/12/13/california_finance_department_lockbit/

https://securityaffairs.co/wordpress/139599/cyber-crime/lockbit-ransomware-california-department-of-finance.html

Russian Hackers Targeted Petroleum Refinery in NATO Country

Source: https://heimdalsecurity.com/blog/russian-hackers-targeted-petroleum-refinery-in-nato-country/

From the Article: "During the ongoing Russo-Ukrainian conflict, the Russian-linked Gamaredon group attempted to break into a large petroleum refining company within NATO member state, on August 30, 2022. The unsuccessful attack, which was attributed to Russia's Federal Security Service (FSB), was just one of multiple intrusions orchestrated by advanced persistent threats (APTs)."

Additional sources:
https://www.cyberscoop.com/russia-hacking-ukraine-nato-energy/

https://industrialcyber.co/ransomware/russia-backed-trident-ursa-group-now-net-widens-to-aim-at-large-petroleum-refining-company-within-nato-nation/

https://arstechnica.com/information-technology/2022/12/kremlin-backed-hackers-

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

targeted-a-large-petroleum-refinery-in-a-nato-nation/

https://thehackernews.com/2022/12/russian-hackers-target-major-petroleum.html

https://therecord.media/russian-hackers-targeted-petroleum-refining-company-in-nato-state/

https://industrialcyber.co/ransomware/russia-backed-trident-ursa-group-now-net-widens-to-aim-at-large-petroleum-refining-company-within-nato-nation/

Rackspace says 'known ransomware group' is behind attack on servers; still working to retrieve data

Source: https://www.expressnews.com/business/article/Rackspace-ransomware-group-17650842.php

From the Article: "In the first interviews since the attack was reported, company executives and an external advisor who's working on the response said they expected their investigations to be completed this week and that they're still trying to restore customers' data."

Additional sources:
https://www.theregister.com/2022/12/14/rackspace_email_outage/

https://www.2-spyware.com/rackspace-hit-by-phishing-and-ransomware-attacks

https://www.techradar.com/news/rackspace-warns-of-phishing-risks-following-ransomware-attack

https://heimdalsecurity.com/blog/rackspace-warns-clients-about-phishing-risks-after-suffering-a-ransomware-attack/

https://www.cybersecuritydive.com/news/rackspace-recover-ransomware-emails/639428/

https://www.expressnews.com/sa-inc/article/Damage-control-Rackspace-ransomware-attack-17672849.php

Play Ransomware Gang Claims Responsibility for Cyber Attack on H-Hotels

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Source: https://www.itsecuritynews.info/play-ransomware-gang-claims-responsibility-for-cyber-attack-on-h-hotels/

From the Article: "H-Hotels (h-hotels.com) have recently been the target of a cyber-attack, which has led to disruptions in the company's communication systems. The Play ransomware gang has claimed responsibility for the attack."

Additional sources:
https://heimdalsecurity.com/blog/play-ransomware-gang-hits-german-hotel-chain/

https://cyberintelmag.com/attacks-data-breaches/cyberattack-on-german-hotel-company-h-hotels-claimed-by-play-ransomware/

https://www.bleepingcomputer.com/news/security/play-ransomware-claims-attack-on-german-hotel-chain-h-hotels/

https://informationsecuritybuzz.com/play-ransomware-gang-claims-cyber-attack-h-hotels/

https://www.malwarebytes.com/blog/news/2022/12/play-ransomware-group-claims-to-have-stolen-h-hotel-data

Another Royal problem: Health department warns of new ransomware threat

Source: https://www.digitaljournal.com/tech-science/another-royal-problem-health-department-warns-of-new-ransomware-threat/article

From the Article: "In recent days the U.S. Department of Health and Human Services (HHS) has issued a warning about 'Royal Ransomware'. Royal is a rapidly growing ransomware operation that is targeting large companies where its ransom demands range from $250,000 to over $2 million."

Additional sources:
https://siliconangle.com/2022/12/14/royal-ransomware-group-attacks-surge-healthcare-prime-target/

https://thecyberwire.com/stories/e3a20645eb3247fd89267d60ba0e1904/warning-on-royal-ransomware-from-hhs

https://healthnews.com/news/new-royal-ransomware-targets-us-healthcare-organizations/

Link back to Table of Contents

https://www.bankinfosecurity.com/royal-ransomware-hitting-healthcare-targets-dumping-data-a-20683

https://thehackernews.com/2022/12/royal-ransomware-threat-takes-aim-at-us.html

Ransomware attack delays SickKids lab results, systems could be offline for weeks

Source: https://torontosun.com/news/local-news/ransomware-attack-delays-sickkids-lab-results-systems-could-be-offline-for-weeks

From the Article: "A ransomware attack has delayed lab and imaging results at Toronto's Hospital for Sick Children and could lead to longer wait times, the hospital said Thursday, noting that some of its systems could be offline for weeks."

Additional sources:
https://www.thestar.com/news/gta/2022/12/22/ransomware-attack-delays-sickkids-lab-results-systems-could-be-offline-for-weeks.html

https://saultonline.com/2022/12/ransomware-attack-delays-sickkids-lab-results-systems-could-be-offline-for-weeks/

https://mobilesyrup.com/2022/12/22/sickkids-ransomware-attack-sickkids-impacted-patient-wait-times/

https://globalnews.ca/video/9368943/ransomware-attack-delays-torontos-sickkids-lab-results-systems-could-be-offline-for-weeks

https://www.thestar.com/news/gta/2022/12/23/sickkids-says-it-could-be-weeks-until-full-recovery-from-ransomware-attack.html

Raspberry Robin Worm Strikes Again, Targeting Telecom and Government Systems

Source: https://thehackernews.com/2022/12/raspberry-robin-worm-strikes-again.html

From the Article: "The Raspberry Robin worm has been used in attacks against telecommunications and government office systems across Latin America, Australia, and Europe since at least September 2022."

Additional sources:
https://securityaffairs.co/wordpress/139964/breaking-news/raspberry-robin-targets-

Link back to Table of Contents

telecom-governments.html

https://industrialcyber.co/ransomware/raspberry-robin-malware-now-targets-telecom-government-entities-in-latin-america-oceania-europe/

https://thehackernews.com/2022/12/raspberry-robin-worm-strikes-again.html

https://www.trendmicro.com/en_us/research/22/l/raspberry-robin-malware-targets-telecom-governments.html

Food Product Shipments Could Be Stolen in BEC Attacks, US Food Companies Warned

Source: https://www.cysecurity.news/2022/12/food-product-shipments-could-be-stolen.html

From the Article: "The US Department of Agriculture (USDA), the Federal Bureau of Investigation (FBI), and the Food and Drug Administration Office of Criminal Investigations (FDA OCI) are all sounding the alarm about business email compromise (BEC) attacks that result in the theft of shipments of food items and ingredients. "

Additional sources:
https://securityaffairs.co/wordpress/139801/cyber-crime/bec-attacks-hijack-shipments-food.html

https://industrialcyber.co/critical-infrastructure/us-agencies-warn-of-hackers-using-bec-tactics-to-steal-large-shipments-of-food-products-ingredients/

https://heimdalsecurity.com/blog/fbi-food-shipments-are-now-the-new-targets-of-bec-attacks/

https://www.darkreading.com/attacks-breaches/fbi-warns-criminals-bec-attacks-steal-food-shipments

Conti associated with Royal ransomware. - CyberWire

Source: https://thecyberwire.com/stories/5730d3e4a5904f07b6b35823589486d4/conti-associated-with-royal-ransomware

From the Article: "Royal ransomware first surfaced in September 2022, and the vast majority of its attacks have targeted entities in the US and Brazil."

Link back to Table of Contents

Additional sources:
https://www.scmagazine.com/brief/ransomware/royal-ransomware-tied-to-conti-gang

https://www.cysecurity.news/2022/12/cybereason-issues-warning-on-rapid.html

https://www.trendmicro.com/en_us/research/22/l/conti-team-one-splinter-group-resurfaces-as-royal-ransomware-wit.html

https://www.securityweek.com/researchers-link-royal-ransomware-conti-group

Lego's BrickLink service narrowly avoids catastrophic API exploit

Source: https://www.itsecurityguru.org/2022/12/15/legos-bricklink-service-narrowly-avoids-catastrophic-api-exploit/

From the Article: "Salt Labs, the research arm of API specialist Salt Security, has revealed it identified a pair of application programming interface (API) security vulnerabilities in Lego's BrickLink digital resale platform. The vulnerabilities have now been fixed."

Additional sources:
https://www.darkreading.com/vulnerabilities-threats/api-flaws-lego-marketplace-user-accounts-data-at-risk

https://news.hitb.org/content/bugs-lego-resale-site-allowed-hackers-hijack-accounts

https://heimdalsecurity.com/blog/lego-tackles-security-flaws-avoids-bricklink-compromise/

https://www.bleepingcomputer.com/news/security/lego-bricklink-bugs-let-hackers-hijack-accounts-breach-servers/

'Russian hackers' help two New York men game JFK taxi system

Source: https://www.cyberscoop.com/russian-hackers-jfk-airport-taxi-scheme/

From the Article: "A pair of men living in New York, working with unnamed Russian nationals, hacked and manipulated the electronic taxis dispatch system at John F. Kennedy International Airport as part of a money-making scheme over a period of at

least two years, federal prosecutors said Tuesday."

Additional sources:
https://www.justice.gov/usao-sdny/pr/two-men-arrested-conspiring-russian-nationals-hack-taxi-dispatch-system-jfk-airport

https://www.securityweek.com/two-men-arrested-jfk-airport-taxi-hacking-scheme

https://www.schneier.com/blog/archives/2022/12/hacking-the-jfk-airport-taxi-dispatch-system.html

https://www.darkreading.com/attacks-breaches/two-indicted-for-hijacking-jfk-airport-taxi-dispatch-

67K Customers Had Their Data Leaked in a Credential Stuffing Attack over DraftKings

Source: https://heimdalsecurity.com/blog/67k-customers-had-their-data-leaked-in-a-credential-stuffing-attack-over-draftkings/

From the Article: "67,995 customers of the sports betting company DraftKings had their personal data exposed in a credential stuffing attack. The incident occurred in November 2022, and it seems that the threat actors got the customers' account credentials from a source outside the organization."

Additional sources:
https://gizmodo.com/draftkings-hackers-sports-gambling-1849911810

https://cyberintelmag.com/attacks-data-breaches/data-breach-at-draftkings-affects-personal-info-of-68000-users/

https://www.securityweek.com/draftkings-data-breach-impacts-personal-information-68000-customers

New Uber Data Breach Exposes Information on 77,000 Employees

Source: https://heimdalsecurity.com/blog/new-uber-data-breach-exposes-information-employees/

From the Article: "Uber suffered a new data breach on December 10th after the "UberLeaks" threat actor spilled stolen data on a notorious hacking forum. "

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Additional sources:
https://www.hackread.com/new-uber-data-breach/

https://www.darkreading.com/attacks-breaches/uber-breached-again-attackers-compromise-third-party-cloud

https://www.bleepingcomputer.com/news/security/uber-suffers-new-data-breach-after-attack-on-vendor-info-leaked-online/

FIN7 Cybercrime Syndicate Emerges as Major Player in Ransomware Landscape

Source: https://thehackernews.com/2022/12/fin7-cybercrime-syndicate-emerges-as.html

From the Article: "An exhaustive analysis of FIN7 has unmasked the cybercrime syndicate's organizational hierarchy, alongside unraveling its role as an affiliate for mounting ransomware attacks."

Additional sources:
https://industrialcyber.co/ransomware/prodaft-details-fin7-cybercrime-gang-exploiting-software-supply-chains-distributing-malicious-usb-sticks/

https://heimdalsecurity.com/blog/fin7-hackers-use-checkmarks-to-exploit-exchange-servers/

https://www.cysecurity.news/2022/12/fin7-cybercrime-syndicate-emerges-as.html

CMS Responds to Third-Party Data Breach Impacting 254K Medicare Beneficiaries

Source: https://healthitsecurity.com/news/cms-responds-to-third-party-data-breach-impacting-254k-medicare-beneficiaries

From the Article: "A third-party data breach potentially impacted the protected health information (PHI) and personally identifiable information (PII) of 254,000 Medicare beneficiaries, the Centers for Medicare & Medicaid Services (CMS) announced. No Medicare claims data were involved, and no CMS systems were breached during the incident."

Additional sources:
https://healthexec.com/topics/health-it/cybersecurity/cms-contractor-data-breach-

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

medicare-beneficiary-data

https://www.healthcareitnews.com/news/cms-subcontractor-hit-ransomware

https://www.hipaajournal.com/up-to-254000-medicare-beneficiaries-affected-by-ransomware-attack-on-cms-subcontractor/

Sophos Thwarts Ransomware Attack by Rare, Malicious Driver Signed with a Valid Digital Certificate

Source: https://www.globenewswire.com/news-release/2022/12/13/2573143/0/en/Sophos-Thwarts-Ransomware-Attack-by-Rare-Malicious-Driver-Signed-with-a-Valid-Digital-Certificate.html

From the Article: "Sophos, a global leader in innovating and delivering cybersecurity as a service, today revealed it has found malicious code in multiple drivers signed by legitimate digital certificates."

Additional sources:
https://www.expresscomputer.in/news/sophos-thwarts-ransomware-attack-by-rare-malicious-driver-signed-with-a-valid-digital-certificate/92771/

https://www.itpro.co.uk/security/malware/369716/ransomware-discovered-carrying-legitimate-windows-certificates

BetMGM Confirms Breach as Hackers Offer to Sell Data of 1.5 Million Customers

Source: https://www.securityweek.com/betmgm-confirms-breach-hackers-offer-sell-data-15-million-customers

From the Article: "MGM Resorts-owned online sports betting company BetMGM confirmed suffering a data breach the same day hackers offered to sell a database containing the information of 1.5 million BetMGM customers."

Additional sources:
https://securityaffairs.co/wordpress/139949/data-breach/betmgm-discloses-security-breach.html

https://www.hackread.com/online-casinos-draftkings-betmgm-hacked/

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Biden signs quantum computing cybersecurity bill into law

Source: https://www.fedscoop.com/biden-signs-quantum-computing-cybersecurity-act-into-law/

From the Article: "President Biden on Wednesday signed legislation to encourage federal government agencies to adopt technology that is protected from decryption by quantum computing."

Additional sources:
https://www.darkreading.com/risk/biden-signs-post-quantum-cybersecurity-guidelines-into-law

https://www.infosecurity-magazine.com/news/biden-quantum-cybersecurity-law/

Glupteba Malware has Returned After Being Disrupted by Google

Source: https://www.cysecurity.news/2022/12/glupteba-malware-has-returned-after.html

From the Article: "After nearly a year of being disrupted by Google, the Glupteba malware botnet has again become active, infecting devices worldwide. As a result of Google's efforts, the blockchain-enabled botnet could be seriously disrupted in December 2021 by securing court orders for control of its infrastructure as well as filing legal claims against two Russian operators. "

Additional sources:
https://thehackernews.com/2022/12/glupteba-botnet-continues-to-thrive.html

https://heimdalsecurity.com/blog/glupteba-malware-is-back-again-heres-what-you-need-to-know/

How ChatGPT can turn anyone into a ransomware and malware threat actor - VentureBeat

Source: https://venturebeat.com/security/chatgpt-ransomware-malware/

From the Article: "Ever since OpenAI launched ChatGPT at the end of November, commentators on all sides have been concerned about the impact AI-driven content-creation will have, particularly in the realm of cybersecurity. In fact, many researchers

Link back to Table of Contents

are concerned that generative AI solutions will democratize cybercrime. "

Additional sources:
https://www.cysecurity.news/2022/12/does-chatgpt-botempower-cyber-crime.html

https://www.infosecurity-magazine.com/news/experts-warn-chatgpt-democratize/

Ransomware Gang Emails College Students with Demands - Campus Safety Magazine

Source: https://www.campussafetymagazine.com/news/ransomware-gang-emails-college-students/

From the Article: "The group, known as the Hive, is believed to be responsible for the attack on the small liberal arts college's computer network, reports NBC News. The hackers sent an email out to students on the evening of December 12."

Additional sources:
https://www.nbcnews.com/tech/security/ransomware-hackers-take-demands-directly-college-students-s-sad-day-rcna61253

Ex-Twitter Worker Gets Prison Time in Saudi 'Spy' Case

Source: https://www.securityweek.com/ex-twitter-worker-gets-prison-time-saudi-spy-case

From the Article: "US justice officials on Thursday said a former Twitter worker convicted of spying for Saudi officials was sentenced to 3.5 years in prison."

Additional sources:
https://thehackernews.com/2022/12/ex-twitter-employee-gets-35-years-jail.html

Clop ransomware group targeting medical images

Source: https://www.beckershospitalreview.com/cybersecurity/clop-ransomware-group-targeting-medical-images.html

From the Article: "Clop, a ransomware group known for its role in the Accellion data breach, has changed its tactics to infect files disguised as medical documents and images, SCMedia reported Dec. 20."

Link back to Table of Contents

Additional sources:
https://www.scmagazine.com/analysis/ransomware/clop-ransomware-group-targeting-provider-patient-trust-by-infecting-medical-images

FINRA sees surge in ransomware attacks - Advisor's Edge

Source: https://www.advisor.ca/news/industry-news/finra-sees-surge-in-ransomware-attacks/

From the Article: ""“Ransomware attacks have proliferated due to, in part, increased use of technology and continued adoption of cryptocurrencies, which bad actors use to hide their identities when collecting ransom payments,” FINRA said in its notice — adding that the availability of attack services on the dark web have enabled attacks on a “much larger scale”."

Additional sources:
https://www.finra.org/rules-guidance/notices/22-29

Intel may delay building Magdeburg fab slated for early 2023

Source: https://www.theregister.com/2022/12/19/intel_german_fab_delay/

From the Article: "No longer 'a definitive date' for facility scheduled to be built from next year"

Additional sources:
https://www.taipeitimes.com/News/biz/archives/2022/12/19/2003790964

Zimperium Reveals Details Of A Newly Discovered Android Threat Campaign That Has Been Stealing Facebook Credentials

Source: https://www.sourcesecurity.com/tags/video-analytics/news/zimperium-reveals-details-newly-discovered-android-co-1641807473-ga.1669957966.html#new_tab

From the Article: "The post Zimperium Reveals Details Of A Newly Discovered Android Threat Campaign That Has Been Stealing Facebook Credentials appeared first on Zimperium."

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Additional sources:
https://www.brighttalk.com/webcast/19320/568541

Meta takes down surveillance-for-hire firms, calls for government action against the industry

Source: https://www.cyberscoop.com/meta-surveillance-for-hire-government-action/

From the Article: "Facebook's parent company Meta barred at least seven companies from the platform over the past year that were involved in surveillance-for-hire activities in an effort to disrupt an industry that's made it increasingly easy to secretly track people online, the company said Wednesday."

Additional sources:
https://www.theguardian.com/technology/2022/dec/15/meta-facebook-owner-warns-spyware-social-media

EarSpy: Spying on Phone Calls via Ear Speaker Vibrations Captured by Accelerometer

Source: https://www.securityweek.com/earspy-spying-phone-calls-ear-speaker-vibrations-captured-accelerometer

Summary: "Previous research focused on vibrations generated by a phone's loudspeakers, or it involved an external component for capturing data. However, an individual is more likely to use the ear speaker rather than the loudspeaker when receiving sensitive information in a phone call."

Additional sources:
https://cyberintelmag.com/attacks-data-breaches/motion-sensors-being-used-in-earspy-attack-to-spy-on-android-phones/

Tata Group to make semiconductor chips in India, invest $90 billion in five years: Report

Source: https://www.news9live.com/technology/tata-group-to-make-semiconductor-chips-in-india-invest-90-billion-in-five-years-report-213421

From the Article: "Tata Group intends to create new projects in developing industries such as electric vehicles. The group will set up a new semiconductor assembly testing business under Tata Electronics. Tata group will look into the prospect of eventually developing an upstream

Link back to Table of Contents

chip fabrication platform."

Incontroller, the intelligent menace

Source: https://www.incibe-cert.es/en/blog/incontroller-intelligent-menace

Summary: PIPEDREAM: Overview of the Pipedream / Incontroller threat environment, components, and tactics used to compromise a system

SVG Files Used by Attackers For Smuggling QBot Malware Onto Windows PCs

Source: https://cyberintelmag.com/malware-viruses/svg-files-used-by-attackers-for-smuggling-qbot-malware-onto-windows-pcs/

Summary: A malware distribution technique using .SVG files (XML based vector graphic) has been identified in the wild. The article suggests disabling javascript or VBScript execution on downloaded material.

Behind the Scenes of Pwn2Own Toronto 2022

Source: https://www.thezdi.com/blog/2022/12/15/behind-the-scenes-of-pwn2own-toronto-2022

Summary: ZDI provides a colorful background into what goes into launching Pwn2Own and handling 85 contestants

WatchGuard Threat Lab Report Finds Top Threat Arriving Exclusively Over Encrypted Connections

Source: https://www.darkreading.com/attacks-breaches/watchguard-threat-lab-report-finds-top-threat-arriving-exclusively-over-encrypted-connections

Summary: It was noted that top malware has started to arrive over encrypted communications, often preventing the snooping of contents being transmitted.

NSA cyber director warns of Russian digital assaults on global energy sector

Link back to Table of Contents

Source: https://www.cyberscoop.com/nsa-energy-sector-cyberattacks/

Summary: ""I would not encourage anyone to be complacent or be unconcerned about the threats to the energy sector globally," Joyce said. "As the [Ukraine] war progresses there's certainly the opportunities for increasing pressure on Russia at the tactical level, which is going to cause them to reevaluate, try different strategies to extricate themselves.""

Dozens of cybersecurity efforts included in this year's US NDAA

Source: https://www.csoonline.com/article/3683469/dozens-of-cybersecurity-efforts-included-in-this-year-s-us-ndaa.html

Summary: A good list of what is included in the FY2023 NDAA, also what is missing, notably SBOMs

CSAF Is the Future of Vulnerability Management

Source: https://www.darkreading.com/threat-intelligence/csaf-is-the-future-of-vulnerability-management

Summary: HIghlights of CSAF and the profiles to help secure software supply chains.

Hacking Using SVG Files to Smuggle QBot Malware onto Windows Systems

Source: https://thehackernews.com/2022/12/hacking-using-svg-files-to-smuggle-qbot.html

Summary: SVG is an XML based image format that can be embedded in HTML files. The SVG may contain scripting code that can be executed as it is loaded.

Lessons Learned From a Forensic Analysis of the Ukrainian Power Grid Cyberattack

Source: https://blog.isa.org/lessons-learned-forensic-analysis-ukrainian-power-grid-cyberattack-malware

Summary: Detailed forensic analysis of how 62443 security levels capability could have

mitigated the attack on the Ukrainian power grid in 2015. From the article: "Looking at the issues listed previously, it appears that raising the SL-A to level 2 would have allowed detection of the activity during step two, thus preventing the cyberattack."

NIST to Retire 27-Year-Old SHA-1 Cryptographic Algorithm

Source: https://www.securityweek.com/nist-retire-27-year-old-sha-1-cryptographic-algorithm

Summary: NIST recommends SHA-1 be replaced with newer and more secure algorithms. SHA-1 is 27 years hold and has been widely broken.

US agencies warn of hackers using BEC tactics to steal large shipments of food products, ingredients

Source: https://industrialcyber.co/critical-infrastructure/us-agencies-warn-of-hackers-using-bec-tactics-to-steal-large-shipments-of-food-products-ingredients/

Summary: Business Email Compromise (BEC) is being used by threat actors to steal food ingredients, impacting the agriculture/food critical infrastructure sector.

GitHub Announces Free Secret Scanning, Mandatory 2FA

Source: https://www.securityweek.com/github-announces-free-secret-scanning-mandatory-2fa

Summary: GitHub is adding features to scan source code of public-facing repositories for secrets (keys, etc.) as well as requiring at least 2FA by the end of 2023.

U.S. to announce fusion energy 'breakthrough'

Source: https://www.washingtonpost.com/business/2022/12/11/fusion-nuclear-energy-breakthrough/

From the Article: "Scientists hit a key milestone in the quest to create abundant zero-carbon power through nuclear fusion. But they still have a long way to go."

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

U.S. asks Japan to help curb China's bid to develop high-end chips

Source: https://www.japantimes.co.jp/news/2022/12/11/business/economy-business/japan-u-s-china-chips/

From the Article: "The United States has directly asked the Japanese government for cooperation in stymieing China's efforts to develop high-end semiconductors, sources familiar with the matter said Saturday."

Using OpenAI Chat to Generate Phishing Campaigns

Source: https://www.richardosgood.com/posts/using-openai-chat-for-phishing/

From the Article: "A classic phishing ruse we use a lot in the industry is the "gift card ruse". The idea is we send an email to the target and entice them to fill out some kind of survey and in return they might win a gift card."

CISA researchers: Russia's Fancy Bear infiltrated US satellite network

Source: https://www.cyberscoop.com/apt28-fancy-bear-satellite/

Summary: "Space security is a growing global concern, especially as key industries and militaries around the world increasingly rely on satellites for vital communications, GPS and internet access. A cyberattack against the U.S. telecom company Viasat, which provides internet service in Europe, disrupted internet service in Ukraine just before the Russian invasion in February."

EVs more issue-prone than gasoline and hybrid cars, Consumer Reports says

Source: https://www.autoblog.com/2022/12/15/evs-electric-cars-reliability-consumer-reports-tesla-model-3-nissan-leaf-kia-ev6/

Summary: It MUST be all the software....

Ukrainian govt networks breached via trojanized Windows 10 installers

Source: https://www.bleepingcomputer.com/news/security/ukrainian-govt-networks-breached-via-trojanized-windows-10-installers/

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Summary: "These malicious installers delivered malware capable of collecting data from compromised computers, deploying additional malicious tools, and exfiltrating stolen data to attacker-controlled servers."

US Puts 3 Dozen More Chinese Companies on Trade Blacklist

Source: https://www.securityweek.com/us-puts-3-dozen-more-chinese-companies-trade-blacklist

Summary: list of companies added to the list.

A Closer Look at Windows Kernel Threats

Source: https://www.trendmicro.com/en_us/research/22/l/a-closer-look-at-windows-kernel-threats.html

Summary: Trend Micro view on Windows Kernel Threats. What are the pros and cons of pursing vulnerabilities in the Kernel vs. ignoring them.

Malicious 'SentinelOne' PyPI package steals data from developers

Source: https://www.bleepingcomputer.com/news/security/malicious-sentinelone-pypi-package-steals-data-from-developers/

Summary: A malicious Python package on PyPi has been published, named 'SentinelOne'. It pretends to be a legitimate SDK for the EDR client of the same name.

The risk of escalation from cyberattacks has never been greater

Source: https://www.wired.com/story/cyberwar-security/

Summary: "In 2023, the world might not get so lucky. There will almost certainly be a major cyberattack. It could shut down Taiwan's airports and trains, paralyze British military computers, or swing a US election."

Link back to Table of Contents

Russian hackers attempted to breach petroleum refining company in NATO country, researchers say

Source: https://www.cyberscoop.com/russia-hacking-ukraine-nato-energy/

Summary: "A Russian-linked hacking group attempted to infiltrate a petroleum refining company in a NATO member state in late August, according to a report by Palo Alto's Unit 42."

Industrial Ammonia Accident Kills One

Source: https://chemical-facility-security-news.blogspot.com/2022/12/industrial-ammonia-accident-kills-one.html

Summary: Possibly an ICS system or safety system is involved that failed to stop the release of ammonia. Investigation pending.

Okta's source code stolen after GitHub repositories hacked

Source: https://www.bleepingcomputer.com/news/security/oktas-source-code-stolen-after-github-repositories-hacked/

Summary: Okta source code stolen from Github

Zerobot IoT Botnet Adds More Exploits, DDoS Capabilities

Source: https://www.securityweek.com/zerobot-iot-botnet-adds-more-exploits-ddos-capabilities

Summary: "Initially detailed two weeks ago, Zerobot is a self-replicating and self-propagating piece of malware written in the Golang (Go) programming language, which can target twelve device architectures."

Over 50 New CVE Numbering Authorities Announced in 2022

Source: https://www.securityweek.com/over-50-new-cve-numbering-authorities-announced-2022

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Summary: There was significant growth in the number of CVE Numbering authorities in 2022. Over 50 new have been added.

DHS, CISA roll out technical rule to update PCII program, bring legal protections for cyber, physical infrastructure information

Source: https://industrialcyber.co/regulation-standards-and-compliance/dhs-cisa-roll-out-technical-rule-to-update-pcii-program-bring-legal-protections-for-cyber-physical-infrastructure-information/

Summary: "For example, some new definitions include ‘CISA,’ ‘Director,’ ‘Executive Assistant Director,’ and ‘PCII Program Manager’ and do not create substantive changes to the regulations."

Two thyssenkrupp divisions targeted in cyberattack, though no data breached

Source: https://industrialcyber.co/news/two-thyssenkrupp-divisions-targeted-in-cyberattack-though-no-data-breached/

Summary: "The spokesperson added that the Group’s IT security (thyssenkrupp Cyber Defense Center) recognised the incident at an early stage and is currently restoring the security of the system.”

It's the anniversary of the worst Crowdstrike report in history

Source: https://jeffreycarr.substack.com/p/its-the-anniversary-of-the-worst

Summary: Overview of the 'Fancy Bear' report in 2016 that Crowdstrike issued, tying Russian Military assets to the DNC hacking over an alleged similarity between the DNC hack and Ukrainian field artillery software on an android phone.

Chinese state-sponsored hacker group RedDelta targeting organizations within Europe, Southeast Asia

Source: https://industrialcyber.co/ransomware/chinese-state-sponsored-hacker-group-reddelta-targeting-organizations-within-europe-southeast-asia/

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Summary: RedDelta is a Chinese linked APT that employs malicious .lnk files to trigger a .DLL search order hijack, updating files that end up compromising the system.

Microsoft Patches Azure Cross-Tenant Data Access Flaw

Source: https://www.securityweek.com/microsoft-patches-azure-cross-tenant-data-access-flaw

Summary: Mnemonic researcher discovered a buggy feature that could allow an Azure customer access beyond their tenet security perimeter

China's ByteDance Admits Using TikTok Data to Track Journalists

Source: https://www.securityweek.com/chinas-bytedance-admits-using-tiktok-data-track-journalists

Summary: ByteDance, parent of TikTok, used data from the TikTok application to track journalists

SentinelLabs details Vice Society ransomware group using custom-branded ransomware payload

Source: https://industrialcyber.co/ransomware/sentinellabs-details-vice-society-ransomware-group-using-custom-branded-ransomware-payload/

Summary: SentinelLabs has disclosed that Vice Society is now using a custom-branded ransomware payload to attack victims.

Prodaft details FIN7 cybercrime gang exploiting software supply chains, distributing malicious USB sticks

Source: https://industrialcyber.co/ransomware/prodaft-details-fin7-cybercrime-gang-exploiting-software-supply-chains-distributing-malicious-usb-sticks/

Summary: FIN7, notorious attack group, cooperates with other threat groups like lockbit, darkside, revil to distribute and develop supply-chain based tools to attack victims

Link back to Table of Contents

For OT Cybersecurity, Extra Time is Running Out

Source: https://www.jdsupra.com/legalnews/for-ot-cybersecurity-extra-time-is-2377700/

Summary: Highlights of TSA railroad security requirements recently enacted.

The permanent Microsoft DCOM hardening patch could shut down your ICS - Industrial Cybersecurity Pulse

Source: https://www.industrialcybersecuritypulse.com/strategies/the-permanent-microsoft-dcom-hardening-patch-could-shut-down-your-ics/?oly_enc_id=7798A4385267C8R

Summary: March 2023, Microsoft will release a permanent DCOM patch that will impact many systems using OPC DA as a communications protocol. Several major vendors have identified this to be an issue and are offering guidance.

Back to work, Linux admins: You have a CVSS 10 kernel bug to address

Source: https://www.theregister.com/2022/12/24/back_to_work_linux_admins/

Summary: Noted issue in the kernel, with a CVSS score of 10.0 around a kernel bug. This particular piece of the kernel is the SMB handling.

How cyber attackers are targeting industrial machines in 2022-2023

Source: https://industrialcyber.co/ransomware/how-cyber-attackers-are-targeting-industrial-machines-in-2022-2023/

Summary: Overview of how attackers are increasingly looking at industrial control systems as potential targets in 2022-2023. Mostly an overview of attacks in 2022 and how the attacks might evolve in 2023.

Log4Shell remains a big threat and a common cause for security breaches

Source: https://www.csoonline.com/article/3684108/log4shell-remains-a-big-threat-and-

Link back to Table of Contents

The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

a-common-cause-for-security-breaches.html

Summary: Long term consequences of Log4Shell and how a common thread is developing in a number of security breaches

Arresting IT Administrators

Source: https://www.schneier.com/blog/archives/2022/12/arresting-it-administrators.html

Summary: Example in Albania of placing IT administrators under house arrest for preventing attacks originating from Iran.

Rethinking VEX

Source: http://tomalrichblog.blogspot.com/2022/12/rethinking-vex.html

Summary: Tom Alrich looks at the reimaging of VEX and how it needs to play in the future ecosystem not only for asset owners but also developers.

NYC's Metropolitan Opera is under cyberattack

Source: https://gothamist.com/news/nycs-metropolitan-opera-is-under-cyberattack

From the Article: " It is the third day of a cyberattack on the Metropolitan Opera that has prevented the institution from selling tickets."

U.S. Could See a Boom in Semiconductor Production | ETF Trends

Source: https://www.etftrends.com/megatrends-channel/u-s-could-see-a-boom-in-semiconductor-production/

From the Article: ""“As the semiconductor manufacturing has truly become vital to the modern economy, there has been a growing consensus to revitalize semiconductor manufacturing in the United States,” said TSMC Chairman Mark Liu during prepared remarks on Tuesday after the President toured the site. “TSMC is also taking a giant step forward to help build a vibrant semiconductor ecosystem in the United States.”"

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Cybersecurity risks in US critical infrastructure sector call for better skills, technologies, processes - Industrial Cyber

Source: https://industrialcyber.co/features/cybersecurity-risks-in-us-critical-infrastructure-sector-call-for-better-skills-technologies-processes/

From the Article: "The industrial cybersecurity sector in 2022 continued to face adversarial attacks in critical infrastructure networks that illustrated knowledge of control system components, industrial protocols, and engineering operations."

In a world first, physicists move light back and forth in time simultaneously

Source: https://interestingengineering.com/science/move-light-back-and-forth-in-time

From the Article: "The experiment could help to form a unified theory of quantum gravity."

Cryptocurrency Mining Campaign Hits Linux Users with Go-based CHAOS Malware

Source: https://thehackernews.com/2022/12/cryptocurrency-mining-campaign-hits.html

From the Article: "A cryptocurrency mining attack targeting the Linux operating system also involved the use of an open source remote access trojan (RAT) dubbed CHAOS."

14 lessons CISOs learned in 2022

Source: https://www.csoonline.com/article/3682748/14-lessons-cisos-learned-in-2022.html

From the Article: "We're about to finish yet another erratic year, in which Elon Musk bought Twitter, Russia invaded Ukraine, and many workers returned to their offices. We also saw, for the first time, a security chief sentenced to prison for concealing a data breach."

White House Names 15 Experts to National Quantum Initiative Advisory Committee

Source: https://thequantuminsider.com/2022/12/10/white-house-names-15-experts-to-national-quantum-initiative-advisory-committee/

From the Article: "The White House announced the appointment of fifteen experts in quantum information science to the National Quantum Initiative Advisory Committee (NQIAC)."

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Indias foreign ministry leaks passport details

Source: https://cybernews.com/security/indias-foreign-ministry-leaks-passport-details/

From the Article: "The Global Pravasi Rishta Portal, India's government platform for connecting with its overseas population, leaked sensitive data, including names and passport details."

12th December – Threat Intelligence Report

Source: https://research.checkpoint.com/2022/12th-december-threat-intelligence-report/

From the Article: "China-linked state-sponsored group Mustang Panda has been using the Russia-Ukraine conflict in a recent phishing campaign, collecting sensitive data from entities in Europe and the Asia Pacific."

Pulling the Curtains on Azov Ransomware: Not a Skidsware but Polymorphic Wiper

Source: https://research.checkpoint.com/2022/pulling-the-curtains-on-azov-ransomware-not-a-skidsware-but-polymorphic-wiper/

From the Article: "During the past few weeks, we have shared the preliminary results of our investigation of the Azov ransomware on social media, as well as with Bleeping Computer. The below report goes into more detail regarding the internal workings of Azov ransomware and its technical features."

From disruption to destruction- Azov Ransomware presents a new shift towards destructive wipers

Source: https://blog.checkpoint.com/2022/12/12/from-disruption-to-destruction-azov-ransomware-presents-a-new-shift-towards-destructive-wipers/

From the Article: "Azov first came to the attention of the information security community as a payload of the SmokeLoader botnet, commonly found in fake pirated software and crack sites. During the past few weeks, Check Point Research (CPR) have shared its preliminary results of investigations into the Azov ransomware on social media, as well as with Bleeping Computer."

TrueBot Malware Employed by Clop Ransomware For Accessing Networks

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Source: https://cyberintelmag.com/malware-viruses/truebot-malware-employed-by-clop-ransomware-for-accessing-networks/

From the Article: "Security experts have observed an increase in the number of computers with the TrueBot malware downloader, developed by the Silence hacking gang that speaks Russian. This group, renowned for its large-scale financial institution heists, has started to move away from using phishing as a first point of breach."

$858 billion defense bill focuses heavily on cyber. These are some highlights.

Source: https://www.cyberscoop.com/cyber-heavy-ndaa-vote/

From the Article: "Congress is poised to vote in coming days on an $858 billion annual defense policy bill that contains significant spending increases for U.S. Cyber Command and other efforts to bolster national cybersecurity defenses."

Australia's Telstra Hit by Data Breach Affected 132,000 Customers

Source: https://www.cysecurity.news/2022/12/australias-telstra-hit-by-data-breach.html

From the Article: "On Sunday, Australia's largest telecom company Telstra Corp Ltd reported that because of an internal technical error 132,000 users' data have been leaked. As per the data, Telstra has 18.8 million customer accounts which is more than the half population of Australia. "

MuddyWater: Iran-Backed Threat Group's Latest Campaign Abuses Syncro Admin Tool

Source: https://www.cysecurity.news/2022/12/muddywater-iran-backed-threat-groups.html

From the Article: "Iran-sponsored cyber threat group, MuddyWater has now altered its tactics, it is now utilizing a remote administration tool, Syncro, that is being used in order to gain control of the target devices. "

5 Methods for Hackers Overcome Cloud Security

Source: https://www.cysecurity.news/2022/12/5-methods-for-hackers-overcome-cloud.html

From the Article: "Nearly every major company has used cloud computing to varying degrees in its operations. To protect against the biggest threats to cloud security, the organization's cloud

Link back to Table of Contents

security policy must be able to handle the integration of the cloud."

Over 4,000 Vulnerable Pulse Connect Secure Hosts Exposed to Internet

Source: https://www.cysecurity.news/2022/12/over-4000-vulnerable-pulse-connect.html

From the Article: "After CISA published a report in April 2021, cautioning online users regarding the exploitations of Pulse Connect secure vulnerabilities, researchers at cybersecurity firm, Censys, found that 4,460 Pulse Connect Secure hosts out of 30,266 appliances exposed to the internet are void of security patches."

Evil Corp-Affiliated Truebot Malware Changes its Strategy to Target RCEs and USBs

Source: https://www.cysecurity.news/2022/12/evil-corp-affiliated-truebot-malware.html

From the Article: "In an advisory released last week, the security firm claims that the campaign it tracked led to the development of two botnets, one with infections spread over the globe (especially in Mexico and Brazil), and the other more recently targeted at the US. "

Chinese Hackers Steal U.S Covid-19 Relief Funds, Experts suspect APT41

Source: https://www.cysecurity.news/2022/12/chinese-hackers-steal-us-covid-19.html

From the Article: "The US Secret Service alleged that a Chinese hacking group stole tens of millions of dollars from US Covid-19 relief funds. The incident has increased the threat that the US and its citizens are facing from threat actors."

Absence of Cybersecurity Expertise Affects Public-Safety Organizations

Source: https://www.cysecurity.news/2022/12/absence-of-cybersecurity-expertise.html

From the Article: "Cybersecurity threats have become pervasive for police departments, first responders, and other public-safety organizations, with 93% of organizations reporting a cybersecurity incident in the previous year. According to a report published on December 8 by cloud platform provider Mark43, which was based on a survey of 343 first responders. "

When Companies Compensate the Hackers, We All Foot the Bill

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Source: https://www.darkreading.com/attacks-breaches/when-companies-compensate-the-hackers-we-all-foot-the-bill

From the Article: "Ensuring stronger in-house defenses is integral to retaining customer loyalty."

Palo Alto Networks Xpanse Active Attack Surface Management Automatically Remediates Cyber Risks Before They Lead to Cyberattacks

Source: https://www.darkreading.com/attacks-breaches/palo-alto-networks-xpanse-active-attack-surface-management-automatically-remediates-cyber-risks-before-they-lead-to-cyberattacks-

From the Article: "New Cortex Xpanse features give organizations visibility and control of their attack surfaces to discover, evaluate, and address cyber risks."

How Do I Use the Domain Score to Determine Whether a Domain Is a Threat?

Source: https://www.darkreading.com/edge-ask-the-experts/how-do-i-use-the-domain-score-to-determine-if-a-domain-is-a-threat

From the Article: "To be most effective, protective DNS services need to constantly reassess and rescore domains as additional data comes in."

95.6% of New Malware in 2022 Targeted Windows

Source: https://www.hackread.com/malware-targeted-windows-2022/

From the Article: "According to researchers, 59.58 million samples of new Windows malware were found in the first three quarters of 2022 and these make up 95.6% of all new malware discovered during that time period. "

CoinTracker - 1,557,153 breached accounts

Source: https://haveibeenpwned.com/PwnedWebsites#CoinTracker

From the Article: "In December 2022, the Crypto & NFT taxes service CoinTracker reported a data breach that impacted over 1.5M of their customers. The company attributed the breach to a compromise of one of their service providers and impacted data was limited to email addresses and partially redacted phone numbers."

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Man Arrested for Hacking NY Hair Salon's POS Provider and Stealing $400K

Source: https://heimdalsecurity.com/blog/man-arrested-for-hacking-ny-hair-salons-pos-provider-and-stealing-400k/

From the Article: "A man from Arizona was detained and charged for hacking into a hair salon chain with its headquarters in New York in order to steal hundreds of thousands of dollars."

COVID-bit: A New Attack Method That Can Breach Air-gapped PCs

Source: https://heimdalsecurity.com/blog/covid-bit-a-new-attack-method-that-can-breach-air-gapped-pcs/

From the Article: "COVID-bit is a new assault strategy that uses electromagnetic waves to breach air-gapped computers, and it has a data transmission range of at least two meters (6.5 ft)."

Unpatched Vulnerabilities Cause Pulse Connect Secure Hosts to Be at Risk

Source: https://heimdalsecurity.com/blog/unpatched-vulnerabilities-cause-pulse-connect-secure-hosts-to-be-at-risk/

From the Article: "Researchers have found more than 4,000 vulnerable Pulse Connect Secure hosts being exposed to the internet. Pulse Connect Secure is a popular remote connectivity VPN solution, which is precisely why it has become the target of attacks from multiple threat actors over time. "

Data Breach Gives Threat Actors Complete Information about Vevor Clients

Source: https://heimdalsecurity.com/blog/data-breach-gives-threat-actors-information-vevor-clients/

From the Article: "A multi-terabyte database belonging to Vevor was left open to the public this year starting July 12th until December. Threat actors had almost five months to feast on the data spillage undisturbed. "

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Clop Ransomware Uses Viral 'Truebot' Malware to Access Networks

Source: https://heimdalsecurity.com/blog/clop-ransomware-uses-viral-truebot-malware-to-access-networks/

From the Article: "Security researchers recently noticed a surge in new devices infected with the Truebot malware downloader. This is created by a Russian-speaking hacking group known as Silence. "

Vulnerability with public PoC affects Cisco IP phones, fix unavailable (CVE-2022-20968)

Source: https://www.helpnetsecurity.com/2022/12/12/cve-2022-20968/

From the Article: "A high-risk stack overflow vulnerability (CVE-2022-20968) may allow attackers to DoS or possibly even execute code remotely on Cisco 7800 and 8800 Series IP phones, the company has confirmed."

Product showcase: The Intruder vulnerability management platform

Source: https://www.helpnetsecurity.com/2022/12/12/product-showcase-intruder-vulnerability-management-platform/

From the Article: "Vulnerability scanning is a fundamental component of every good cyber security strategy – but it can be challenging to get right. Intruder created a vulnerability management platform to make it simple and save time, so that every business can enjoy the same level of security as banks and governments worldwide but without the complexity."

Preventing a ransomware attack with intelligence: Strategies for CISOs

Source: https://www.helpnetsecurity.com/2022/12/12/preventing-a-ransomware-attack-with-intelligence-strategies-for-cisos/

From the Article: "Bad news first: Ransomware isn't going anywhere. The good news? The right intelligence can help organizations dramatically reduce risk surrounding a cyber extortion event. "

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Week in review: Rackspace outage, Kali Linux 2022.4 released, Patch Tuesday forecast

Source: https://www.helpnetsecurity.com/2022/12/11/week-in-review-rackspace-outage-kali-linux-2022-4-released-patch-tuesday-forecast/

From the Article: "Here's an overview of some of last week's most interesting news, articles, interviews and videos: Rackspace Hosted Exchange outage was caused by ransomware Rackspace has finally confirmed the cause of the security incident that resulted in an ongoing outage of its Hosted Exchange service: it's ransomware. "

DHS Secretary Mayorkas addresses convergence of national and homeland security, amidst volatile threat landscape

Source: https://industrialcyber.co/critical-infrastructure/dhs-secretary-mayorkas-addresses-convergence-of-national-and-homeland-security-amidst-volatile-threat-landscape/

From the Article: "U.S. Department of Homeland Security (DHS) secretary Alejandro Mayorkas recently spoke of the convergence of national security and homeland security. He also addressed how the nation faces a new kind of warfare, which is no longer constrained by borders or military maneuvers. "

Nozomi throws light on security vulnerabilities found in Winbox payload protocol used to configure MikroTik devices

Source: https://industrialcyber.co/vulnerabilities/nozomi-throws-light-on-security-vulnerabilities-found-in-winbox-payload-protocol-used-to-configure-mikrotik-devices/

From the Article: "Researchers from industrial cybersecurity firm Nozomi Networks released Friday technical analysis of the core of the Meris botnet capabilities. The team identified that from about 2018 to 2021, the Glupteba botnet, the backbone of the Meris botnet, has been used to infect and turn hundreds of thousands of MikroTik devices into nefarious internet relays."

Cybersecurity risks in US critical infrastructure sector call for better skills, technologies, processes

Source: https://industrialcyber.co/features/cybersecurity-risks-in-us-critical-infrastructure-sector-call-for-better-skills-technologies-processes/

Link back to Table of Contents

From the Article: "The industrial cybersecurity sector in 2022 continued to face adversarial attacks in critical infrastructure networks that illustrated knowledge of control system components, industrial protocols, and engineering operations."

North Korean Hackers Impersonate Researchers to Steal Intel

Source: https://www.infosecurity-magazine.com/news/north-korean-hackers-researchers/

From the Article: "Report associates new intelligence-gathering tactic with Kimsuky group."

Royal Ransomware Targets US Healthcare

Source: https://www.infosecurity-magazine.com/news/royal-ransomware-targets-us/

From the Article: "Requested ransom payment demands ranged from $250,000 to over $2m."

Chaos RAT Used to Enhance Linux Cryptomining Attacks

Source: https://www.infosecurity-magazine.com/news/chaos-rat-used-linux-cryptominingva/

From the Article: "The main downloader script and further payloads were hosted in different locations."

A week in security (December 5 - 11)

Source: https://www.malwarebytes.com/blog/news/2022/12/a-week-in-security-december-5-11

From the Article: "Security advisories are falling short. Here's why, with Dustin Childs: Lock and Code S03E25."

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Iranian hacking group uses compromised email accounts to distribute MSP remote access tool

Source: https://www.malwarebytes.com/blog/news/2022/12/iranian-hacking-group-uses-compromised-email-accounts-to-distribute-msp-remote-access-tool

From the Article: "Researchers have uncovered a new campaign by hacking group MuddyWater, aka Static Kitten, in which a legitimate remote access tool is sent to targets from a compromised email account."

Users Warned of New Aerst, ScareCrow, and Vohuk Ransomware Families - SecurityWeek

Source: https://www.securityweek.com/users-warned-new-aerst-scarecrow-and-vohuk-ransomware-families

From the Article: "Targeting Windows computers, these are typical ransomware families that encrypt victim files and demand a ransom payment in exchange for a decryption key. This new ransomware has been used in an increasing number of attacks."

Royal Ransomware Targets US Healthcare - Infosecurity Magazine

Source: https://www.infosecurity-magazine.com/news/royal-ransomware-targets-us/

From the Article: "The ransomware group known as Royal has been targeting the healthcare industry in the US, warned the Health Department (HC3) last week."

CommonSpirit ransomware attack exposed personal information of 623K people, system says

Source: https://www.healthcaredive.com/news/commonspirit-ransomware-attack-patient-information-623k/638500/

From the Article: "CommonSpirit Health has told regulators that the protected health information of more than 623,700 people was comprised in a ransomware attack first announced in October."

Link back to Table of Contents

Truebot Malware Adopts New Tactics, Ramps Up Operations - Spiceworks

Source: https://www.spiceworks.com/it-security/security-general/news/truebot-downloader-malware-attacks-rising/

From the Article: "Researchers at Talos, Cisco's threat intelligence arm, also linked Truebot creator Silence group to the notorious Evil Corp (TA505). The Talos advisory suggests there exist two different Truebot campaigns leveraging two different botnets that drop various payloads, including Grace (or FlawedGrace and GraceWire), Cobalt Strike and Clop ransomware, both of which are associated with Evil Corp."

PLAY ransomware group claims responsibility for Antwerp attack as second Belgian city ...

Source: https://therecord.media/play-ransomware-group-claims-responsibility-for-antwerp-attack-as-second-belgian-city-confirms-new-incident/

From the Article: "The PLAY ransomware group has claimed responsibility for a ransomware attack on the Belgian city of Antwerp last week, just as the city of Diest about an hour's drive east confirmed on Monday that it has been hit by a cyberattack."

The pros of proactive cyber risk protection | Insurance Business America

Source: https://www.insurancebusinessmag.com/us/news/cyber/the-pros-of-proactive-cyber-risk-protection-430331.aspx

From the Article: "Last month, the Toronto-based global cyber insurance specialist BOXX Insurance acquired the cyber threat intelligence platform Templarbit – a company whose technology enables companies to learn if their network has vulnerabilities that hackers can exploit."

Enterprise Ransomware Protection Rising Growth | Bitdefender, Sophos, Avast

Source: https://www.drinksmediawire.com/enterprise-ransomware-protection-rising-growth-bitdefender-sophos-avast/

From the Article: "Market Reports recently broadcasted a new study in its database that highlights the in-depth market analysis with future prospects of Enterprise Ransomware Protection market."

Link back to Table of Contents

Rackspace Hit With Lawsuits Over Ransomware Attack | SecurityWeek.Com

Source: https://www.securityweek.com/rackspace-hit-lawsuits-over-ransomware-attack

From the Article: "Rackspace's Hosted Exchange environment started experiencing problems on December 2. The firm revealed one day later that it was dealing with a security incident that forced it to shut down its hosted Microsoft Exchange service."

Truesec and Europol partner to fight cybercrime - IBS Intelligence

Source: https://ibsintelligence.com/ibsi-news/truesec-and-europol-partner-to-fight-cybercrime/

From the Article: "Cybersecurity companies Truesec and Europol have joined forces to disrupt criminal businesses with the initiative "No More Ransom". As part of the initiative, Truesec has developed a unique decryption tool that will help ransomware victims to recover encrypted files, without having to pay cybercriminals."

Nonprofit-led ransomware task force seeks federal efforts to disrupt payment cycle, more ...

Source: https://insidecybersecurity.com/daily-news/nonprofit-led-ransomware-task-force-seeks-federal-efforts-disrupt-payment-cycle-more

From the Article: "The Institute for Security and Technology's Ransomware Task Force is highlighting its accomplishments over the past 18 months, while offering areas for continued collaboration in disrupting the payment structure and international engagements."

TrueBot infections were observed in Clop ransomware attacks - Security Affairs

Source: https://securityaffairs.co/wordpress/139527/malware/truebot-infections-clop-ransomware-attacks.html

From the Article: "Cisco Talos researchers reported an increase in TrueBot infections, threat actors have shifted from using malicious emails as their primary attack vector to

other techniques."

Hackers Shut Down The Government Systems Of An Entire State For A Month - Vanuatu

Source: https://technewsspace.com/hackers-shut-down-the-government-systems-of-an-entire-state-for-a-month-vanuatu/

From the Article: "Cyberattacks on government information systems have become fairly commonplace across the world, but it has recently become clear that such activities by intruders can cripple the workings of an entire country's IT infrastructure. For a month, the Pacific island nation of Vanuatu suffered from the actions of criminals."

Mitigating Ransomware is Not Simple and We Recommend a 4-Layer Protection

Source: https://www.cxotoday.com/cxo-bytes/mitigating-ransomware-is-not-simple-and-we-recommend-a-4-layer-protection/

From the Article: "Enterprises can take advantage of Trend Micro Vision One™, which collects and correlates data across endpoints, emails, cloud workloads and networks, providing better context and enabling investigation in one place."

Cybersecurity Landscape 2023: Upcoming Trends And Risks - BW Businessworld

Source: https://www.businessworld.in/article/Cybersecurity-Landscape-2023-Upcoming-Trends-And-Risks/12-12-2022-457593

From the Article: "The year 2022 will be remembered as the year when battle lines were drawn, then redrawn, along a threat landscape stuck in a state of in-between. No longer are enterprises scrambling to find their footing amid the disruption caused by Covid-19, but for all this talk of the "new normal," the world has yet to arrive on the other side of the pandemic."

Latest Cyberattack on LJ Hooker by a Ransomware Gang | IT Security News

Source: https://www.itsecuritynews.info/latest-cyberattack-on-lj-hooker-by-a-ransomware-gang/

Link back to Table of Contents

From the Article: "It is reported that a ransomware gang has been able to steal the personal data of at least 375 gigabytes from a franchise of the Australian real estate giant, LJ Hooker, as a result of its ransomware attacks."

AIIMS Delhi Ransomware Attack Was Deliberate, Targeted; NIA Probe Underway, MoS IT Says

Source: https://samacharcentral.com/aiims-delhi-ransomware-attack-was-deliberate-targeted-nia-probe-underway-mos-it-says/

From the Article: "The National Investigation Agency (NIA) is investigating the “deliberate and targeted” ransomware attack on the servers of AIIMS Delhi, Minister of State for IT Rajeev Chandrasekhar said on Thursday."

When Cyber Criminals Come for the Courts and Hack Justice

Source: https://www.governing.com/security/when-cyber-criminals-come-for-the-courts-and-hack-justice

From the Article: "Serious cyber incidents struck state courts in Alaska, Georgia and Texas in the past couple years, with one leaving Alaska’s courts a month without Internet and four months without connection to the executive branch."

What Is Threat Intelligence? Definition and Examples

Source: https://www.recordedfuture.com/threat-intelligence-definition

From the Article: "If youre new to the field, or you think your organization could benefit from a carefully constructed threat intelligence program, heres what you need to know first."

Cryptomining campaign targets Linux systems with Go-based CHAOS Malware

Source: https://securityaffairs.co/wordpress/139554/cyber-crime/cryptocurrency-mining-campaign-chaos-malware.html

From the Article: "In November 2022, Trend Micro researchers discovered a

cryptocurrency mining campaign targeting Linux users with Go-based CHAOS malware (Trojan.Linux.CHAOSRAT)."

Evilnum group targets legal entities with a new Janicab variant

Source: https://securityaffairs.co/wordpress/139540/hacking/evilnum-new-janicab-variant.html

From the Article: "Kaspersky researchers reported that a hack-for-hire group dubbed Evilnum is targeting travel and financial entities. The attacks are part of a campaign aimed at legal and financial investment institutions in the Middle East and Europe."

Security Affairs newsletter Round 397

Source: https://securityaffairs.co/wordpress/139513/breaking-news/security-affairs-newsletter-round-397.html

From the Article: "A new round of the weekly SecurityAffairs newsletter arrived! Every week the best security articles from Security Affairs free for you in your email box."

MuddyWater APT group is back with updated TTPs

Source: https://securityaffairs.co/wordpress/139505/apt/muddywater-changs-ttps.html

From the Article: "The Iran-linked MuddyWater APT is targeting countries in the Middle East as well as Central and West Asia in a new campaign."

How The Talent Shortage Changes the Approach to Cybersecurity

Source: https://securityintelligence.com/articles/how-talent-shortage-changes-cybersecurity/

From the Article: "There’s good news, and there’s bad news. The good news is that the number of cybersecurity professionals has reached an all-time high. According to (ISC)2’s annual Cybersecurity Workforce Study, 4.7 million people currently work in a security-related job. "

Link back to Table of Contents

Researchers Demonstrate How EDR and Antivirus Can Be Weaponized Against Users

Source: https://thehackernews.com/2022/12/researchers-demonstrate-how-edr-and.html

From the Article: "High-severity security vulnerabilities have been disclosed in different endpoint detection and response (EDR) and antivirus (AV) products that could be exploited to turn them into data wipers."

Washington's semiconductor sanctions won't slow China's military build-up | The Strategist

Source: https://www.aspistrategist.org.au/washingtons-semiconductor-sanctions-wont-slow-chinas-military-build-up/

From the Article: "Now that advanced semiconductors are seen as essential to national defence, Beijing is adopting a 'whole of the nation' approach and investing national resources into the industry."

Apple Will Use Chips Made in the USA

Source: https://techacute.com/apple-will-use-chips-made-in-the-usa/

From the Article: "A change is coming soon in Apple because they will be using US-made microchips in their product. The CEO Tim Cook confirmed the upcoming expansion of the company at an event by Taiwan Semiconductor Manufacturing Company's (TSMC) "tool-in" ceremony last week."

Mobile Threat Patterns Across Sweden | 2022 Q3 Analysis

Source: https://www.brighttalk.com/webcast/19320/566218

From the Article: "The post Mobile Threat Patterns Across Sweden | 2022 Q3 Analysis appeared first on Zimperium."

Link back to Table of Contents

Precious Gemstones: The New Generation of Kerberos Attacks

Source: https://unit42.paloaltonetworks.com/next-gen-kerberos-attacks/

From the Article: "Unit 42 researchers show new methods to improve detection of a next-gen line of Kerberos attacks, which allow attackers to modify Kerberos tickets to maintain privileged access."

Linux Cryptocurrency Mining Attacks Enhanced via CHAOS RAT

Source: https://www.trendmicro.com/en_us/research/22/l/linux-cryptomining-enhanced-via-chaos-rat-.html

From the Article: "We intercepted a cryptocurrency mining attack that incorporated an advanced remote access trojan (RAT) named the CHAOS Remote Administrative Tool."

UK arrests five for selling 'dodgy' point of sale software

Source: https://www.theregister.com/2022/12/12/j5_electronic_sales_suppression_software_probe/

From the Article: "Tax authorities from Australia, Canada, France, the UK and the USA have conducted a joint probe into "electronic sales suppression software" – applications that falsify point of sale data to help merchants avoid paying tax on their true revenue."

Using threat modeling to get your priorities right

Source: https://www.theregister.com/2022/12/12/red_canary_threat_modeling_promo1/

From the Article: "How does your security team prioritize work? When a new attack from a state actor hits the news, do you know if your team should drop everything to hunt for IOCs? Do you understand your security control coverage for the threat actors that might target your organization?"

Japan, Australia, to bolster cyber-defenses, maybe offensive capacity too

Link back to Table of Contents

Source: https://www.theregister.com/2022/12/11/asia_tech_news_roundup/

From the Article: "Australia's home affairs and cybersecurity minister Clare O'Neill has given the nation a goal of becoming the world's most cyber secure nation by 2030."

Top 4 SaaS Security Threats for 2023

Source: https://thehackernews.com/2022/12/top-4-saas-security-threats-for-2023.html

From the Article: "With 2022 coming to a close, there is no better time to buckle down and prepare to face the security challenges in the year to come. This past year has seen its fair share of breaches, attacks, and leaks, forcing organizations to scramble to protect their SaaS stacks."

Cryptocurrency Mining Campaign Hits Linux Users with Go-based CHAOS Malware

Source: https://thehackernews.com/2022/12/cryptocurrency-mining-campaign-hits.html

From the Article: "The threat, which was spotted by Trend Micro in November 2022, remains virtually unchanged in all other aspects, including when it comes to terminating competing malware, security software, and deploying the Monero (XMR) cryptocurrency miner."

Criminal ransomware updates. Iranian cyberattacks. A night at the opera. Notes on the hybrid war.

Source: https://thecyberwire.com/newsletters/daily-briefing/11/236

From the Article: "TrueBot found in Cl0p ransomware attacks. Royal ransomware targets the healthcare sector. Recent Iranian cyber activity. Update on the cyberattack against the Metropolitan Opera."

Recent Iranian cyber operations.

Source: https://thecyberwire.com

From the Article: "Discussion of Iranian cyber operations, with particular attention to the

Agrius and MuddyWater threat groups."

What Happens When the Metaverse Enters Your Attack Surface?
Source: https://www.tenable.com/blog/what-happens-when-the-metaverse-enters-your-attack-surface

From the Article: "Here at Tenable, we often discuss the challenges faced by cybersecurity professionals as they grapple with protecting an ever-expanding attack surface that includes on-premises infrastructure as well as public and private clouds, identity and privilege management systems and web applications. Soon to be added to that mix: the metaverse."

Tenable Cyber Watch: Shift Left Challenges, Anti-Ransomware Efforts, Quantum Risks and CISO Anxiety
Source: https://www.tenable.com/blog/tenable-cyber-watch-shift-left-challenges-anti-ransomware-efforts-quantum-risks-and-ciso

From the Article: "Beat the Monday blues with cyber news you can use | Shift-left efforts falling short. The White House's war on ransomware. Everything you've ever wanted to know about CISOs. The quantum computing risk for critical infrastructure."

12 Days of Cybersecurity – Part 2
Source: https://blog.blueyonder.com/12-days-of-cybersecurity-part-2/

From the Article: "They see you when you're sleeping, they know when you're awake, they're cyber-criminals and they're everywhere. No need to fear, cybersecurity is here with Part 2 of our 12 Days of Cybersecurity. Pour yourself a glass of eggnog, throw on your coziest slippers and enjoy these next six cybersecurity tips. And in case you missed it, you can check out Part 1 here."

Python, JavaScript Developers Targeted With Fake Packages Delivering Ransomware
Source: https://www.securityweek.com/python-javascript-developers-targeted-fake-packages-delivering-ransomware

From the Article: "Phylum security researchers warn of a new software supply chain attack relying on typosquatting to target Python and JavaScript developers."

Link back to Table of Contents

Fortinet Ships Emergency Patch for Already-Exploited VPN Flaw
Source: https://www.securityweek.com/fortinet-ships-emergency-patch-already-exploited-vpn-flaw

From the Article: "Fortinet on Monday issued an emergency patch to cover a severe vulnerability in its FortiOS SSL-VPN product, warning that hackers have already exploited the flaw in the wild."

Device Exploits Earn Hackers Nearly $1 Million at Pwn2Own Toronto 2022
Source: https://www.securityweek.com/device-exploits-earn-hackers-nearly-1-million-pwn2own-toronto-2022

From the Article: "The Zero Day Initiative's Pwn2Own Toronto 2022 hacking contest has come to an end, with participants earning nearly $1 million for exploits targeting smartphones, printers, routers, NAS devices, and smart speakers."

IT threat evolution Q3 2022
Source: https://securelist.com/it-threat-evolution-q3-2022/107957/

From the Article: "In July, we reported a rootkit that we found in modified Unified Extensible Firmware Interface (UEFI) firmware, the code that loads and initiates the boot process when the computer is turned on. Rootkits are malware implants that are installed deep in the operating system."

War in Ukraine Dominated Cybersecurity in 2022 - CNET
Source: https://www.cnet.com/tech/services-and-software/war-in-ukraine-dominated-cybersecurity-in-2022/

From the Article: "Russia's war against Ukraine and the worries about possible cyberattacks against the country's allies, like the US, dominated cybersecurity news throughout 2022."

Pentagon, private sector must partner to fight new era of cyberattacks - Federal Times
Source: https://www.c4isrnet.com/cyber/2022/12/12/pentagon-private-sector-must-partner-to-fight-new-era-of-cyberattacks/

From the Article: "It takes constant communication to enhance the efficacy of public and private sector entities in detecting and mitigating cyberattacks on everything from

federal systems and critical infrastructure to banks and hospitals."

Travis Central Appraisal District restores services one week after ransomware attack
Source: https://cbsaustin.com/news/local/travis-central-appraisal-district-restores-services-one-week-after-ransomware-attack

From the Article: "One week after being hit with a ransomware attack, the Travis Central Appraisal District (TCAD) says its customer services to property owners have been restored."

CommonSpirit Ransomware Breach Affects About 624,000 So Far - BankInfoSecurity
Source: https://www.bankinfosecurity.com/commonspirit-ransomware-breach-affects-about-624000-so-far-a-20689

From the Article: "The second-largest nonprofit hospital chain in the United States has slowly dribbled out information about the ransomware attack it first detected in early October (see: Patients Affected by Cybersecurity Event at Hospital Chain)."

TrueBot malware delivery evolves, now infects businesses in the US and elsewhere
Source: https://www.techrepublic.com/article/truebot-malware-delivery-evolution/

From the Article: "According to Cisco Talos, TrueBot malware now collects Active Directory information, which means it targets businesses with larger IT resources. In addition to targeting larger organizations, the malware is experimenting with new delivery methods: Netwrix Auditor bundled with the Raspberry Robin malware."

From Counties to Banks: Tracing the Footprint of Ransomware Attack IoCs - CircleID
Source: https://circleid.com/posts/20221212-from-counties-to-banks-tracing-the-footprint-of-ransomware-attack-iocs

From the Article: "SecurityScorecard published a report on a cyber attack that a U.S. county victim announced on 11 September 2022. With ransomware attacks against local government units increasing in the past few years, WhoisXML API researchers decided to build on the list of IP addresses related to the attacks."

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Travis County appraisal district's operations restored after ransomware attack
Source: https://www.statesman.com/story/news/2022/12/12/austin-travis-county-appraisal-district-restored-after-ransomware-attack/69720717007/

From the Article: "A week after falling victim to a ransomware attack, the Travis Central Appraisal District has been able to fully restore its customer service operations, agency officials said Monday."

ALMA still recovering from devastating cyberattack - Physics Today
Source: https://physicstoday.scitation.org/do/10.1063/PT.6.2.20221212a/full/

From the Article: "More than a month after a ransomware cyberattack on its computer systems, the Atacama Large Millimeter/Submillimeter Array (ALMA) in Chile remains offline. The unprecedented disruption is hindering the research projects of astronomers around the world and is costing the observatory about a quarter of a million dollars a day."

TYO detects nearly 11 million cyber security threats in Qatar - Trade Arabia
Source: http://www.tradearabia.com/news/IT_404149.html

From the Article: "Trend Micro Incorporated (TYO), a global leader in cybersecurity solutions, predicts that ransomware groups will increasingly target Linux servers and embedded systems over the coming years. The latest Trend Micro 2022 Midyear Roundup Report recorded a double-digit year-on-year (YoY) increase in attacks on these systems in H1 2022."

Cyber Attacks: Better Safe Than Sorry [Indian Currents] - InsuranceNewsNet
Source: https://insurancenewsnet.com/oarticle/cyber-attacks-better-safe-than-sorry-indian-currents

From the Article: "About a fortnight back, that is on November 23, several patient-related e-services like appointments, registrations, smart billing, admission, discharge, report generation, etc., were reportedly affected at All India Institute of Medical Sciences (AIIMS) Delhi. "

Morgan County School District Re-3 canceled classes on Friday in wake of cybersecurity incident
Source:

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

https://www.google.com/url?rct=j&sa=t&url=https://www.databreaches.net/morgan-county-school-district-re-3-canceled-classes-on-friday-in-wake-of-cybersecurity-incident/&ct=ga&cd=CAIyGmY5NWQ3ZDU3NzU5MmRlMjE6Y29tOmVuOlVT&usg=AOvVaw34wAKUm5GnndQn-oiZJU7D

From the Article: "Morgan County Schools recently discovered a cybersecurity incident impacting its network environment. We are currently working with a team of forensic experts to fully understand the extent and implications of this incident and to restore operations within a safe and remediated network environment. We apologize for the operational disruption that this event may have caused, or continue to cause, until a safe restoration of services has been completed."

Malaysia launches investigation into low-cost airline Air Asia ransomware attack - YouTube
Source: https://www.google.com/url?rct=j&sa=t&url=https://www.youtube.com/watch%3Fv%3D9pLtG0db2l0&ct=ga&cd=CAIyGmY5NWQ3ZDU3NzU5MmRlMjE6Y29tOmVuOlVT&usg=AOvVaw1Rg2fqEKvEgGKIGd6cAapR

From the Article: "Last month, a ransomware attack compromised the personal data of approximately five million passengers and all Air Asia employees."

HSE Cyber-Attack Costs Ireland $83m So Far
Source: https://www.infosecurity-magazine.com/news/hse-cyber-attack-ireland-dollar83m/

From the Article: "A total of roughly 100,000 people had their personal data stolen during the cyber-attack."

The Outlook for Strategic Competition in the Semiconductor Industry
Source: https://www.wilsoncenter.org/event/outlook-strategic-competition-semiconductor-industry

From the Article: "Growing strategic competition between China and the United States is manifesting itself clearly in the semiconductor industry. Alongside attempts to diversify its semiconductor supply chain away from Taiwan, the US is also trying to slow the development of China's national semiconductor industry. Recent export controls announced by the Biden administration have already begun to have an effect on China's industry, and more actions are expected to follow."

Link back to Table of Contents

Global chip industry projected to invest more than 500 billion in new factories by 2024 semi reports
Source: https://www.semi.org/en/news-media-press-releases/semi-press-releases/global-chip-industry-projected-to-invest-more-than-$500-billion-in-new-factories-by-2024-semi-reports

From the Article: "MILPITAS, Calif. — December 12, 2022 — The worldwide semiconductor industry is projected to invest more than $500 billion in 84 volume chipmaking facilities starting construction from 2021 to 2023, with segments including automotive and high-performance computing fueling the spending increases, SEMI announced today in its latest quarterly World Fab Forecast report. The projected growth in global factory count includes a record high 33 new semiconductor manufacturing facilities starting construction this year and 28 more in 2023."

Singapore PMI summary as of November 2022 - SIPMM PMI
Source: https://pmi.sipmm.edu.sg/pmi-nov-2022/

From the Article: "The November reading of the Singapore Purchasing Managers' Index (PMI) increased 0.1 point from the previous month to post a third month of continuous contraction at 49.8. The latest PMI reading was attributed to a slower contraction in the key indexes of new orders, factory output and inventory."

US lawmakers introduce bill to ban TikTok
Source: https://www.cnn.com/2022/12/13/tech/tiktok-ban-bill/index.html

From the Article: "Washington(CNN)A trio of US lawmakers has introduced new legislation that aims to ban TikTok from operating in the United States. The new bill by Sen. Marco Rubio, the top Republican on the Senate Intelligence Committee, and a bipartisan pair of congressmen in the House, reflects the latest escalation by US policymakers against the Chinese-owned short-form video app. TikTok has faced doubts about its ability to safeguard US user data from the Chinese government."

Chinese chip designers slow down processors to dodge US sanctions
Source: https://www.ft.com/content/7df13a5e-84e8-44af-b0d3-3e3efa6a8671

From the Article: "Cutting-edge semiconductor companies tweak specifications to comply with export controls"

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

China's Semiconductor Industry Is About to Suffer Another Major Blow
Source: https://www.pcmag.com/news/chinas-semiconductor-industry-is-about-to-suffer-another-major-blow

From the Article: "Japan and the Netherlands are expected to agree to only supply China with machines capable of producing 14nm chips, which are three generations behind the state-of-the-art semiconductors."

New Actively Exploited Zero-Day Vulnerability Discovered in Apple Products
Source: https://thehackernews.com/2022/12/new-actively-exploited-zero-day.html

From the Article: "Apple on Tuesday rolled out security updates to iOS, iPadOS, macOS, tvOS, and Safari web browser to address a new zero-day vulnerability that could result in the execution of malicious code."

The State of the Transistor in 3 Charts
Source: https://spectrum.ieee.org/transistor-density

From the Article: "In 75 years, it's become tiny, mighty, ubiquitous, and just plain weird"

Global Chip Industry Projected to Invest More Than $500 Billion in New Factories by 2024, SEMI Reports
Source: https://www.prnewswire.com/news-releases/global-chip-industry-projected-to-invest-more-than-500-billion-in-new-factories-by-2024-semi-reports-301699188.html

From the Article: "MILPITAS, Calif., Dec. 12, 2022 /PRNewswire/ -- The worldwide semiconductor industry is projected to invest more than $500 billion in 84 volume chipmaking facilities starting construction from 2021 to 2023, with segments including automotive and high-performance computing fueling the spending increases, SEMI announced today in its latest quarterly World Fab Forecast report. The projected growth in global factory count includes a record high 33 new semiconductor manufacturing facilities starting construction this year and 28 more in 2023."

Despite DOE's efforts, cybersecurity threats to US electric sector continue to evolve, needing more efforts to manage risk - Industrial Cyber
Source: https://industrialcyber.co/features/despite-does-efforts-cybersecurity-threats-to-us-electric-sector-continue-to-evolve-needing-more-efforts-to-manage-risk/?

From the Article: "The U.S. electric sector continues to be an attractive target for

cyberattacks from adversaries and individual bad actors, such as insiders and cyber criminals. Nations and criminal groups pose the most significant cyber threats to U.S. critical infrastructure, according to the Director of National Intelligence's 2022 Annual Threat Assessment. Additionally, these hackers are increasingly capable of attacking the grid."

Indian government issues SOP to employees on Cyber Attacks - Cybersecurity Insiders
Source: https://www.cybersecurity-insiders.com/indian-government-issues-sop-to-employees-on-cyber-attacks/

From the Article: "Central government employees of India will receive a Standard Operating Procedure (SOP) on Cyber Attacks by this month and suggesting measures to take before a cyber attack and steps to mitigate risks, if in case, an organization becomes a victim to a digital attack."

Samsung Electronics $4.8 billion Texas tax break approved
Source: https://koreajoongangdaily.joins.com/2022/12/14/business/tech/Korea-Samsung-Electroncis-TSMC/20221214182011132.html

From the Article: "Samsung Electronics has received approval for $4.8 billion of tax breaks in Texas for planned and proposed semiconductor plants."

Challenges With Adaptive Control
Source: https://semiengineering.com/challenges-with-adaptive-control/

From the Article: "Systems are becoming more attuned to their operational environment, but this adds many questions and issues that need to be resolved."

Cybersecurity: Trends From 2022 And Predictions For 2023
Source: https://www.infosecurity-magazine.com/blogs/trends-from-2022-predictions-for/

From the Article: "As our home networks continue to merge with the enterprise, and as enterprises across all industries become more dispersed, cybersecurity threats increase. Along with ongoing digital transformation and the proliferation of cloud, that dispersal introduces new challenges for the cybersecurity community. The past 12 months have proven that adapting hasn't been easy."

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Keith Krach on Weaponizing Trust - The Wire China
Source: https://www.thewirechina.com/2022/12/11/keith-krach-on-weaponizing-trust/

From the Article: "The business veteran and former State Department official talks about pushing back against Huawei; 'tech statecraft'; and fighting back when the market is no longer free."

US scientists reach long-awaited nuclear fusion breakthrough, source says
Source: https://www.cnn.com/2022/12/12/politics/nuclear-fusion-energy-us-scientists-climate/index.html

From the Article: "(CNN)For the first time ever, US scientists at the National Ignition Facility at the Lawrence Livermore National Laboratory in California successfully produced a nuclear fusion reaction resulting in a net energy gain, a source familiar with the project confirmed to CNN."

Hackers Actively Exploiting Citrix ADC and Gateway Zero-Day Vulnerability

Source: https://thehackernews.com/2022/12/hackers-actively-exploiting-citrix-adc.html

From the Article: "The U.S. National Security Agency (NSA) on Tuesday said a threat actor tracked as APT5 has been actively exploiting a zero-day flaw in Citrix Application Delivery Controller (ADC) and Gateway to take over affected systems."

U.S. announces nuclear fusion energy breakthrough: "One of the most impressive scientific feats of the 21st century"

Source: https://www.cbsnews.com/news/nuclear-fusion-energy-breakthrough-announcement/

From the Article: "The U.S. Department of Energy announced Tuesday a monumental milestone in nuclear fusion research: a "net energy gain" was achieved for the first time in history by scientists from the Lawrence Livermore National Laboratory in California."

Google Launches OSV-Scanner Tool to Identify Open Source Vulnerabilities

Source: https://thehackernews.com/2022/12/google-launches-largest-distributed.html

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

From the Article: "Google on Tuesday announced the open source availability of OSV-Scanner, a scanner that aims to offer easy access to vulnerability information about various projects."

Global total semiconductor equipment sales 2022

Source: https://www.semi.org/en/news-media-press/semi-press-releases/global-total-semiconductor-equipment-sales-2022

From the Article: "TOKYO — December 13, 2022 — Global sales of total semiconductor manufacturing equipment by original equipment manufacturers are forecast to reach a new high of $108.5 billion in 2022, rising 5.9% from the previous industry record of $102.5 billion in 2021, SEMI announced today in its Year-End Total Semiconductor Equipment Forecast – OEM Perspective at SEMICON Japan 2022."

Analysis: China's massive older chip tech buildup raises U.S. concern

Source: https://www.reuters.com/technology/chinas-massive-older-chip-tech-build-up-raises-us-concern-2022-12-13/

From the Article: "China's largest chim maker SMIC is raming up production of a decade-old chip technology, key to many industries' supply chains, setting off alarm bells in the United States and prompting some lawmakers to try to stop them."

ENISA reports on Cyber Europe 2022, tests business continuity and crisis management across EU healthcare sector - Industrial Cyber

Source: https://industrialcyber.co/medical/enisa-reports-on-cyber-europe-2022-tests-business-continuity-and-crisis-management-across-eu-healthcare-sector/

From the Article: "The European Union Agency for Cybersecurity (ENISA) published on Tuesday an ‘after action’ report of Cyber Europe 2022, the cybersecurity exercise aimed at testing the resilience of the region’s healthcare sector."

Fortinet Warns of Active Exploitation of New SSL-VPN Pre-auth RCE Vulnerability

Source: https://thehackernews.com/2022/12/fortinet-warns-of-active-exploitation.html

Link back to Table of Contents

From the Article: "Fortinet on Monday issued emergency patches for a severe security flaw affecting its FortiOS SSL-VPN product that it said is being actively exploited in the wild."

China Weighs Over $143B In Semiconductor Push To Beat US Embargo

Source: https://finance.yahoo.com/news/china-weighs-over-143b-semiconductor-125932907.html

From the Article: "China earmarked over 1 trillion yuan ($143 billion) in support package for its semiconductor industry, in a significant step towards self-sufficiency in chips and to counter the U.S. embargo."

SEC Charges Samuel Bankman-Fried with Defrauding Investors in Crypto Asset Trading Platform FTX

Source: https://www.sec.gov/news/press-release/2022-219

From the Article: "Defendant concealed his diversion of FTX customers' funds to crypto trading firm Alameda Research while raising more than $1.8 billion from investors"

DOE National Laboratory Makes History by Achieving Fusion Ignition

Source: https://www.energy.gov/articles/doe-national-laboratory-makes-history-achieving-fusion-ignition

From the Article: "For First Time, Researchers Produce More Energy from Fusion Than Was Used to Drive It, Promising Further Discovery in Clean Power and Nuclear Weapons Stewardship"

An open call to the visionaries in government to change DoD culture

Source: https://www.defensenews.com/opinion/commentary/2022/12/12/an-open-call-to-the-visionaries-in-government-to-change-dod-culture/

From the Article: "Clearly, there's an issue that even some top DoD leaders can't ignore.

Link back to Table of Contents

I strongly suspect there's a growing consensus among some of the rank and file across the DoD that something has to give."

How The Talent Shortage Changes the Approach to Cybersecurity

Source: https://securityintelligence.com/articles/how-talent-shortage-changes-cybersecurity/

From the Article: "There's good news, and there's bad news. The good news is that the number of cybersecurity professionals has reached an all-time high. According to (ISC)2's annual Cybersecurity Workforce Study, 4.7 million people currently work in a security-related job."

LA Semiconductor Purchases Fabrication Plant From onsemi

Source: https://www.manufacturing.net/operations/news/22604667/la-semiconductor-purchases-fabrication-plant-from-onsemi

From the Article: "LA Semiconductor will run the fab as a pure-play contract manufacturing foundry."

High Voltage Testing Races Ahead

Source: https://semiengineering.com/high-voltage-testing-races-ahead/

From the Article: "Testing SiC and GaN devices evolves with the market, but gaps remain."

TPG Telecom joins list of hacked Australian companies, shares slide

Source: https://www.reuters.com/world/asia-pacific/tpg-telecom-finds-evidence-unauthorised-access-up-15000-email-accounts-2022-12-13/

From the Article: "Internet services provider TPG Telecom Ltd became the latest Australian company to fall victim to a high-profile cyberattack, announcing on Wednesday that the emails of up to 15,000 of its corporate customers had been accessed."

Link back to Table of Contents

Malware Strains Targeting Python and JavaScript Developers Through Official Repositories

Source: https://thehackernews.com/2022/12/malware-strains-targeting-python-and.html

From the Article: "An active malware campaign is targeting the Python Package Index (PyPI) and npm repositories for Python and JavaScript with typosquatted and fake modules that deploy a ransomware strain, marking the latest security issue to affect software supply chains."

U.S. Semiconductor Export Controls on the PRC: Prospects for Success

Source: https://www.nbr.org/publication/u-s-semiconductor-export-controls-on-the-prc-prospects-for-success/

From the Article: "In October the U.S. Department of Commerce's Bureau of Industry and Security released an unprecedented set of export controls targeting the semiconductor industry in the People's Republic of China (PRC)."

NSA Releases Series on Protecting DoD Microelectronics From Adversary Influence

Source: https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3239938/nsa-releases-series-on-protecting-dod-microelectronics-from-adversary-influence/

From the Article: "FORT MEADE, Md. — The National Security Agency's Joint Federated Assurance Center (JFAC) Hardware Assurance Lab publicly released four Cybersecurity Technical Reports today to help the Department of Defense protect field-programmable gate array (FPGA)-based systems from adversary influence."

Improving Chip Efficiency, Reliability, And Adaptability

Source: https://semiengineering.com/improving-chip-efficiency-reliability-and-adaptability/

From the Article: "Fraunhofer IIS EAS' director maps out a plan for the next generation

of electronics."

Cybersecurity Experts Uncover Inner Workings of Destructive Azov Ransomware

Source: https://thehackernews.com/2022/12/cybersecurity-experts-uncover-inner.html

From the Article: "Cybersecurity researchers have published the inner workings of a new wiper called Azov Ransomware that's deliberately designed to corrupt data and "inflict impeccable damage" to compromised systems."

The CHIPS Act Has Already Sparked $200 Billion in Private Investments for U.S. Semiconductor Production

Source: https://www.semiconductors.org/the-chips-act-has-already-sparked-200-billion-in-private-investments-for-u-s-semiconductor-production/

From the Article: "From the time the CHIPS Act was introduced in the Spring of 2020 through the months following its enactment, companies in the semiconductor ecosystem announced dozens of projects to increase manufacturing capacity in the U.S."

Nascio 2023 cio top 10

Source: https://www.nascio.org/press-releases/nascio-2023-cio-top-10/

From the Article: "LEXINGTON, Ky., Monday, December 12, 2022—Today, the National Association of State Chief Information Officers (NASCIO) released the State CIO Top 10 for 2023. The Top 10 represents state technology leaders' top policy and technology priorities for the coming year, as voted on by 51 state and territory chief information officers (CIOs), and has been published every year since 2007."

State cio top ten policy and technology priorities for 2023

Source: https://www.nascio.org/resource-center/resources/state-cio-top-ten-policy-and-technology-priorities-for-2023/

From the Article: "NASCIO conducts a survey of the state CIOs to identify and prioritize the top policy and technology issues facing state government. The CIOs top ten

priorities are identified and used as input to NASCIO's programs, planning for conference sessions, and publications."

IBM partners with Japan's Rapidus in bid to manufacture advanced chips

Source: https://www.reuters.com/technology/ibm-partners-with-new-japanese-chip-maker-rapidus-make-advanced-chips-2022-12-13/

From the Article: "TOKYO/OAKLAND, Calif, Dec 13 (Reuters) - IBM Corp and Rapidus, a newly formed chip maker backed by the Japanese government, on Tuesday announced a partnership that aims to manufacture the world's most advanced chips in Japan by the second half of the decade."

Quantum-ready workforce tops White House, scientists' list of needs

Source: https://www.fedscoop.com/quantum-ready-workforce-david-awschalom/

From the Article: "Workforce was the topic on most quantum scientists' minds when 30 of the country's best met at the White House on Dec. 2 to discuss the global quantum race."

New GoTrim Botnet Attempting to Break into WordPress Sites' Admin Accounts

Source: https://thehackernews.com/2022/12/new-gotrim-botnet-attempting-to-break.html

From the Article: "A new Go-based botnet has been spotted scanning and brute-forcing self-hosted websites using the WordPress content management system (CMS) to seize control of the targeted systems."

National security updates en route as Quantum Computing Cybersecurity Preparedness Act passes Congress - Homeland Preparedness News

Source: https://homelandprepnews.com/stories/79288-national-security-updates-en-route-as-quantum-computing-cybersecurity-preparedness-act-passes-congress/

From the Article: "Following its passage from the Senate last week, the Quantum

Computing Cybersecurity Preparedness Act officially navigated both chambers of Congress, setting up changes to national security through new quantum computer defenses if signed into law by President Joe Biden."

Global semiconductor industry outlook for 2023

Source: https://advisory.kpmg.us/articles/2022/global-semiconductor-industry-outlook-2023.html

From the Article: "Leaders optimistic about growth, driven by automotive and the end of the chip shortage"

Microsoft report finds attackers use multiple tactics, approaches to target OT, as critical infrastructure risks rise - Industrial Cyber

Source: https://industrialcyber.co/it-ot-collaboration/microsoft-report-finds-attackers-use-multiple-tactics-approaches-to-target-ot-as-critical-infrastructure-risks-rise/?

From the Article: "A new Microsoft report provided new insights on wider risks that converging IT, Internet of Things (IoT), and operational technology (OT) systems pose to critical infrastructure. The data reported a spike in the presence of attackers across these environments and networks fueled by the convergence and interconnectivity many organizations have adopted over the past few years."

Lehi's Texas Instruments facility begins semiconductor production - Lehi Free Press

Source: https://lehifreepress.com/2022/12/13/lehis-texas-instruments-facility-begins-semiconductor-production/

From the Article: "Texas Instruments (TI) announced the official start of semiconductor production at its Lehi campus on December 6, 2022. Lehi's facility, or "LFAB," as TI labels it, is the second semiconductor manufacturing facility owned by TI to commence 300-mm wafer production in 2022, about one year after the company purchased the facility from Micron. "

GPS Signals Are Being Disrupted in Russian Cities

Link back to Table of Contents

Source: https://www.wired.com/story/gps-jamming-interference-russia-ukraine/

From the Article: "Navigation system monitors have seen a recent uptick in interruptions since Ukraine began launching long-range drone attacks. "

CHIPS Act scorebook: 4 Taiwan firms investing US$45.5 billion to create 6,200 jobs in America

Source: https://www.digitimes.com/news/a20221215VL206/sia-taiwan-us.html

From the Article: "The Semiconductor Industry Association (SIA) compiled a list of semiconductor-related investment projects announced between the time the CHIPS Act was introduced in the Spring of 2020 through the months following its enactment, showing that a total of US$200 billion of investment has been made across 16 states and will increase 40,000 jobs directly."

TSMC Founder Morris Chang Is Wrong, Globalization (Only) Needs a Reset | The Ojo-Yoshida Report

Source: https://ojoyoshidareport.com/tsmc-founder-morris-chang-is-wrong-globalization-only-needs-a-reset/

From the Article: "Globalization is alive and well but requires a reality check--and fine tuning."

Tsmc announces big expansion plans for anticipated arizona fab

Source: https://www.allaboutcircuits.com/news/tsmc-announces-big-expansion-plans-for-anticipated-arizona-fab/

From the Article: "TSMC will be adding a second fab to its Phoenix, Arizona, site—with plans to make both 4 nm and 3 nm process chips within the next three years."

Experts urge jamming detection network – Free webinar shows easy method using smartphones - GPS World

Source: https://www.linkedin.com/pulse/experts-urge-jamming-detection-network-free-

webinar-shows-goward

From the Article: "By all accounts, it is getting worse. Hundreds of internet sites sell inexpensive devices to interfere with GPS and other GNSS signals. Estimates place the number of devices extant in the United States in the tens of thousands or more."

How the Decades-Long Chinese Espionage Campaign "Stole" US Military Technology

Source: https://warriormaven.com/china/chinese-espionage-stole-us-military-technology

From the Article: "Many US-driven technological advances may have been stolen by Chinese spies"

Bringing Next-Generation eBeam Technology Out of the Lab and into the Fab

Source: https://www.appliedmaterials.com/content/applied-materials/us/en/blog/blog-posts/bringing-next-generation-ebeam-technology-out-of-the-lab-and-into-the-fab

UMC approves capital appropriation plan for fabs in Tainan, Singapore - Focus Taiwan

Source: https://focustaiwan.tw/sci-tech/202212150009

From the Article: "Taipei, Dec. 15 (CNA) United Microelectronics Corp. (UMC), the second largest contract chipmaker in Taiwan, has approved capital appropriations of more than NT$32 billion (US$1.05 billion) to expand a fab in Tainan and build another fab in Singapore."

ASU, Mexico partner to boost semiconductor production in N. America

Source: https://www.todaysmedicaldevelopments.com/article/semiconductor-arizona-state-university-mexico-mou/

From the Article: "Mexican ambassador visits Arizona State University to talk about the CHIPS Act, tour facilities, sign memorandum of understanding."

Link back to Table of Contents

Collaboration key to fueling sustainable chip industry growth to over 1 trillion by 2030 semicon europa 2022 highlights

Source: https://www.semi.org/en/blogs/semi-news/collaboration-key-to-fueling-sustainable-chip-industry-growth-to-over-$1-trillion-by-2030-semicon-europa-2022-highlights

From the Article: "Among the topics discussed were accelerating innovation through collaborative research and development, creating a roadmap for greener and more trusted applications and the role semiconductors play in doing so, and challenges and opportunities in manufacturing excellence and global supply chain optimization."

2023 Cybersecurity predictions

Source: https://cybersecurity.att.com/blogs/security-essentials/2023-cybersecurity-predictions

From the Article: "Cybersecurity is a relatively new discipline in the realm of computing. Once computing became more democratized with PCs connected via local area networks (LAN) and client/server environments, adversaries quickly saw opportunities."

Impacts Facing The Supply Chain Ahead of the Holiday Season

Source: https://www.allthingssupplychain.com/impacts-facing-the-supply-chain-ahead-of-the-holiday-season/

From the Article: "Supply chain issues have negatively affected companies worldwide since early 2020. The COVID-19 pandemic brought restrictions and changed policies for businesses, leading to shortages in supplies and workers."

Anomali Cyber Watch: MuddyWater Hides Behind Legitimate Remote Administration Tools, Vice Society Tops Ransomware Threats to Education, Abandoned JavaScript Library Domain Pushes Web-Skimmers

Source: https://www.anomali.com/blog/anomali-cyber-watch-muddywater-hides-behind-legitimate-remote-administration-tools-vice-society-tops-ransomware-threats-to-education-abandoned-javascript-library-domain-pushes-web-skimmers

From the Article: "The various threat intelligence stories in this iteration of the Anomali

Cyber Watch discuss the following topics: APT, Compromised websites, Education, Healthcare, Iran, Phishing, Ransomware, and Supply chain."

MoneyMonger: Predatory Loan Scam Campaigns Move to Flutter

Source: https://www.zimperium.com/blog/moneymonger-predatory-loan-scam-campaigns-move-to-flutter/

From the Article: "Flutter, the open-source user interface (UI) software kit for cross-platform mobile applications, has helped drive new mobile applications onto the market. This modern mobile application framework removes many barriers to creating multi-platform applications, and developers can create native mobile apps with only one codebase."

Schoolyard Bully Trojan Facebook Credential Stealer

Source: https://www.zimperium.com/blog/schoolyard-bully-trojan-facebook-credential-stealer/

From the Article: "Zimperium zLabs has discovered a new Android threat campaign, the Schoolyard Bully Trojan, which has been active since 2018. The campaign has spread to over 300,000 victims and is specifically targeting Facebook credentials. "

Multiple Vulnerabilities in Apple Products Could Allow for Arbitrary Code Execution

Source: https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-apple-products-could-allow-for-arbitrary-code-execution_2022-145

From the Article: "Multiple vulnerabilities have been discovered in Apple Products, the most severe of which could allow for arbitrary code execution."

Multiple Vulnerabilities in Adobe Products Could Allow for Arbitrary Code Execution.

Source: https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-adobe-products-could-allow-for-arbitrary-code-execution_2022-143

From the Article: "Multiple vulnerabilities have been discovered in Adobe products, the

most severe of which could allow for arbitrary code execution."

Multiple Vulnerabilities in Google Chrome Could Allow for Arbitrary Code Execution

Source: https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-google-chrome-could-allow-for-arbitrary-code-execution_2022-144

From the Article: "Multiple vulnerabilities have been discovered in Google Chrome, the most severe of which could allow for arbitrary code execution. Google Chrome is a web browser used to access the internet. Successful exploitation of the most severe of these vulnerabilities could allow for arbitrary code execution in the context of the logged on user."

A vulnerability has been discovered in Citrix Gateway and Citrix ADC which could allow for remote code execution

Source: https://www.cisecurity.org/advisory/a-vulnerability-has-been-discovered-in-citrix-gateway-and-citrix-adc-which-could-allow-for-remote-code-execution_2022-142

From the Article: "A vulnerability has been discovered in Citrix Gateway and Citrix ADC which could allow for remote code execution. Citrix ADC and Gateway is an Application Delivery Controller and a gateway service to products respectively. Successful exploitation of this vulnerability could allow an unauthenticated remote attacker to perform arbitrary code execution. "

Multiple Vulnerabilities in VMware vRealize Network Insight (vRNI) Could Allow for Arbitrary Code Execution

Source: https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-vmware-vrealize-network-insight-vrni-could-allow-for-arbitrary-code-execution_2022-141

From the Article: "Multiple vulnerabilities have been discovered in VMware vRealize Network Insight (vRNI), the most severe of which could result in arbitrary code execution. VMware vRealize Network Insight (vRNI) is an IT management platform which enables visibility, optimization and management of an organization’s physical, virtual and cloud infrastructure."

Link back to Table of Contents

Multiple Vulnerabilities in Mozilla Products Could Allow for Arbitrary Code Execution

Source: https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-mozilla-products-could-allow-for-arbitrary-code-execution_2022-140

From the Article: "Multiple vulnerabilities have been discovered in Mozilla Firefox, Firefox Extended Support Release (ESR) and Mozilla Thunderbird, the most severe of which could allow for arbitrary code execution."

A Vulnerability in Fortinet's FortiOS Could Allow for Arbitrary Code Execution

Source: https://www.cisecurity.org/advisory/a-vulnerability-in-fortinets-fortios-could-allow-for-arbitrary-code-execution_2022-139

From the Article: "A vulnerability has been discovered in Fortinet's FortiOS, which could allow for arbitrary code Execution. FortiOS is the Fortinet's proprietary Operation System which is utilized across multiple product lines. "

November 2022's Most Wanted Malware: A Month of Comebacks for Trojans as Emotet and Qbot Make an Impact

Source: https://blog.checkpoint.com/2022/12/13/november-2022s-most-wanted-malware-a-month-of-comebacks-for-trojans-as-emotet-and-qbot-make-an-impact/

From the Article: "Check Point Research reports that Emotet has returned after a quiet summer, now the second most prevalent malware globally. "

Threat Source newsletter (Dec. 15, 2022): Talos Year in Review is here

Source: https://blog.talosintelligence.com/threat-source-newsletter-dec-15-2022-christmas-came-early/

From the Article: "It's the most wonderful time of the year, and I'm not talking about the holidays. The inaugural 2022 Talos Year in Review is here! And it's taking over the final Threat Source newsletter of the year. Oh and did we mention we're on Mastodon now? Talos, the gift that keeps on giving."

Link back to Table of Contents

Vulnerability Spotlight: Denial-of-service vulnerability discovered in VMWare vCenter

Source: https://blog.talosintelligence.com/vulnerability-spotlight-denial-of-service-vulnerability-discovered-in-vmware-vcenter/

From the Article: "Cisco Talos recently discovered a denial-of-service vulnerability in VMWare vCenter Server."

Syncovery For Linux Web-GUI Authenticated Remote Command Execution

Source: https://packetstormsecurity.com/files/170245/syncovery_linux_rce_2022_36534.rb.txt

From the Article: "This Metasploit module exploits an authenticated command injection vulnerability in the Web GUI of Syncovery File Sync and Backup Software for Linux. Successful exploitation results in remote code execution under the context of the root user."

MTTR "not a viable metric" for complex software system reliability and security

Source: https://www.csoonline.com/article/3683508/mttr-not-a-viable-metric-for-complex-software-system-reliability-and-security.html

From the Article: "Mean time to resolve (MTTR) isn't a viable metric for measuring the reliability or security of complex software systems and should be replaced by other, more trustworthy options. "

Dozens of cybersecurity efforts included in this year's US NDAA

Source: https://www.csoonline.com/article/3683469/dozens-of-cybersecurity-efforts-included-in-this-year-s-us-ndaa.html

From the Article: "Last week, members of the US House of Representatives and Senate reconciled their versions of the annual must-pass National Defense Authorization Act (NDAA). Each year the NDAA contains a wealth of primarily military cybersecurity provisions, delivering hundreds of millions, if not billions, in new cybersecurity funding to the federal government."

Link back to Table of Contents

New Royal ransomware group evades detection with partial encryption

Source: https://www.csoonline.com/article/3682854/new-royal-ransomware-group-evades-detection-with-partial-encryption.html

From the Article: "A new ransomware group dubbed Royal that formed earlier this year has significantly ramped up its operations over the past few months and developed its own custom ransomware program that allows attackers to perform flexible and fast file encryption."

Palo Alto Networks flags top cyberthreats, offers new zero-day protections

Source: https://www.csoonline.com/article/3682754/palo-alto-networks-flags-top-cyberthreats-offers-new-zero-day-protections.html

From the Article: "Firewall and security software vendor Palo Alto Network's annual Ignite conference kicked off Tuesday, highlighted by several product announcements, which were unveiled alongside the company's latest threat report."

BrandPost: Staying Cyber Safe This Holiday Season with Security Awareness Training

Source: https://www.csoonline.com/article/3682753/staying-cyber-safe-this-holiday-season-with-security-awareness-training.html

From the Article: "The holiday season is the most wonderful time of the year for cybercriminals. Threat adversaries inevitably have more opportunities to carry out targeted attacks as more people are online shopping and checking emails for coupons that could actually be phishing attacks."

SVG Files Used by Attackers For Smuggling QBot Malware Onto Windows PCs

Source: https://cyberintelmag.com/malware-viruses/svg-files-used-by-attackers-for-smuggling-qbot-malware-onto-windows-pcs/

From the Article: "A novel distribution technique for QBot malware phishing campaigns uses SVG files to smuggle HTML and produce malicious Windows installation locally."

Link back to Table of Contents

New Backdoor in Python Found, Targets VMware ESXi Servers

Source: https://cyberintelmag.com/malware-viruses/new-backdoor-in-python-found-targets-vmware-esxi-servers/

From the Article: "According to Juniper Networks' Threat Labs security experts, a new Python-based backdoor that targets VMware ESXi virtualization servers has been discovered."

NSA cyber director warns of Russian digital assaults on global energy sector

Source: https://www.cyberscoop.com/nsa-energy-sector-cyberattacks/

From the Article: "National Security Agency Cyber Director Rob Joyce said Thursday he remains concerned about significant cyberattacks from Russia, warning that Moscow could unleash digital assaults on the global energy sector in the coming months."

NSA says Chinese hackers are actively attacking flaw in widely used networking device

Source: https://www.cyberscoop.com/citrix-china-apt5-hackers/

From the Article: "The National Security Agency said on Tuesday that Chinese state-backed hackers are exploiting a flaw in a widely used networking device that allows an attacker to carry out remote code execution. "

Iranian hacking group expands focus to US politicians, critical infrastructure, researchers find

Source: https://www.cyberscoop.com/iran-ta453-charming-kitten-phosphorus-hacking-bolton/

From the Article: "An Iranian hacking group previously thought to mainly focus on compromising academics, journalists and human rights workers now appears to have included U.S. politicians, critical infrastructure and medical researchers to its target list, according to the cybersecurity firm Proofpoint."

Unveiling CrowdStrike Falcon Surface: The Industry's Most Complete Adversary-Driven

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

External Attack Surface Management (EASM) Technology

Source: http://provinggrounds.cs.sys/blog/crowdstrike-falcon-surface-adversary-driven-external-attack-surface-management-technology/

From the Article: "As the attack surface expands, so does the “community” of adversaries and cybercriminals exploiting externally exposed assets to break into organizations around the globe."

Why Managed Threat Hunting Should Top Every CISO’s Holiday Wish List

Source: http://provinggrounds.cs.sys/blog/managed-threat-hunting-should-top-every-ciso-wish-list/

From the Article: "With the end of the year fast approaching, many of us are looking forward to a well-deserved break. However, security practitioners and security leaders worldwide are bracing themselves for what has become a peak period for novel and disruptive threats. "

Attackers Set Sights on Active Directory: Understanding Your Identity Exposure

Source: http://provinggrounds.cs.sys/blog/attackers-set-sights-on-active-directory-understanding-your-identity-exposure/

From the Article: "Eighty percent of modern attacks are identity-driven. Why would an attacker hack into a system when they can simply use stolen credentials to masquerade as an approved user and log in to the target organization? "

CrowdStrike Services Helps Organizations Prioritize Patching Vulnerabilities with CrowdStrike Falcon Spotlight

Source: http://provinggrounds.cs.sys/blog/how-to-leverage-crowdstrike-falcon-spotlight-to-prioritize-vulnerabilities/

From the Article: "When the CrowdStrike Services team conducts a proactive security engagement, such as a Cybersecurity Maturity Assessment or Tabletop Exercise, it often uses CrowdStrike Falcon® Spotlight to identify what vulnerabilities exist in the environment."

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Hackers can Overcome Air-Gapped Systems to Steal Data

Source: https://www.cysecurity.news/2022/12/hackers-can-overcomeair-gapped-systems.html

From the Article: "An air gap is a safety feature that isolates a computer or network and prevents it from connecting to the outside world. A computer that is physically isolated and air-gapped is unable to communicate wirelessly or physically with some other computers or network components. "

Email Hack Hits 15,000 Business Customers of TPG

Source: https://www.cysecurity.news/2022/12/email-hack-hits-15000-business.html

From the Article: "The second largest Australian telecommunications company TPG fell victim to a high-profile cyber attack. TPG is Australia's No. 2 Internet service provider which serves 7.2 million accounts in the nation. TPG Telecom was previously known as Vodafone Hutchison Australia, however, it was renamed after its merger with TPG. "

Hackers can Hijack Antivirus Software to Erase Data

Source: https://www.cysecurity.news/2022/12/hackers-can-hijack-antivirus-software.html

From the Article: "In a report released this week, a top cybersecurity researcher revealed that many popular antivirus software programs had been exploited, for their ability to erase data, including Microsoft, SentinelOne, TrendMicro, Avast, and AVG. "

What is Zero Trust Architecture and How it Reduces Cyberthreat Risks?

Source: https://www.cysecurity.news/2022/12/what-is-zero-trust-architecture-and-how.html

From the Article: "For the past thirty years, organizations have been focusing on establishing and optimizing complex, wide-area, and hub-and-spoke networks in order to connect online users and company branches to the data center over private networks. "

Link back to Table of Contents

LockBit Latest Variant LockBit 3.0, With BlackMatter Capabilities

Source: https://www.cysecurity.news/2022/12/lockbit-latest-variant-lockbit-30-with.html

From the Article: "Healthcare sectors' cybersecurity intelligence has been requested to review the IOCs and has also been recommended to take proactive steps to fight against BlackCat and LockBit 3.0 ransomware variants which are rampantly targeting healthcare sectors. "

Users' Data was Breached in 2021, Twitter Confirms

Source: https://www.cysecurity.news/2022/12/users-data-was-breached-in-2021-twitter.html

From the Article: "A Twitter spokesperson confirmed that the breach that affected millions of users' profiles, including private phone numbers and email addresses, was indeed caused by the same data breach that Twitter disclosed in August 2022, in which millions of emails and phone numbers were obtained."

24 Percent of Technology Applications Have High-risk Security Vulnerabilities

Source: https://www.cysecurity.news/2022/12/24-percent-of-technology-applications.html

From the Article: "With a higher proportion of applications to compete with than other industries, technology firms would benefit from improving secure coding training and practices for their development teams. As per Veracode, 24 percent of applications in the technology sector contain high-risk security flaws, which would cause a critical issue for the application if exploited. "

An Active Typosquat Attack in PyPI and NPM Discovered

Source: https://www.cysecurity.news/2022/12/an-active-typosquat-attack-in-pypi-and.html

From the Article: "The typosquatting-based software supply chain threat, which targets

explicitly Python and JavaScript programmers, is being warned off by Phylum security researchers."

Threat Actors Distribute Around 400K Malicious Files Every-day to Attack Users

Source: https://www.cysecurity.news/2022/12/threat-actors-distribute-around-400k.html

From the Article: "According to one of the latest reports, nearly 4,00,000 new malicious files were apparently distributed every day by threat actors in the year 2022, in order to deceive and attack online users. The report shows a significant 5 percent growth compared to the 2021 data of the same. "

AirAsia Ransomware Attack Affected 5 Million People, Investigated in Malaysia

Source: https://www.cysecurity.news/2022/12/airasia-ransomware-attack-affected-5.html

From the Article: "It was announced last month that approximately five million AirAsia passengers, as well as all of the company's employees, were affected by a ransomware attack. Malaysian authorities have yet to find the source of the attack and determine the overall impact but have gathered few leads so far."

Is Malware The Reason Your Smartphone Keyboard is Not Working?

Source: https://www.cysecurity.news/2022/12/is-malware-reason-your-smartphone.html

From the Article: "Most problems, faced when a smartphone is not functioning properly, can be resolved by resetting the device, deleting the cache, or installing an alternative keyboard app. But, what if none of that is helpful?"

Phishing: The Biggest Security Threat of 2023

Source: https://www.cysecurity.news/2022/12/phishing-biggest-security-threat-of-2023.html

From the Article: "The year is about to end and every year we are witnessing that cybercriminals are advancing their methods of attacking systems and networks.

Link back to Table of Contents

Therefore there are various reasons why private firms and federal agencies should be more prepared for the coming years. As per the recent analysis Phishing attacks will be the greatest security threat in 2023. "

Attackers Can Still Exploit Log4j Vulnerability to Track Activities

Source: https://www.cysecurity.news/2022/12/attackers-can-still-exploit-log4j.html

From the Article: "Countless digital goods and services have been affected internationally since December 1, 2021, as a vulnerability related to the open-source logging framework Apache Log4j 2 has been aggressively abused. "

Cyberattack on the City of Antwerp's Servers Triggered via PLAY Ransomware

Source: https://www.cysecurity.news/2022/12/cyberattack-on-city-of-antwerps-servers.html

From the Article: "The IT, email, and phone services in Antwerp were interrupted last week as a result of a ransomware attack on Digipolis, the IT firm in charge of overseeing the city's IT infrastructure."

For More Than a Month, a Cyberattack has Kept an Entire Nation's Government Offline

Source: https://www.cysecurity.news/2022/12/for-more-than-month-cyberattack-has.html

From the Article: "Cyberattacks on government institutions are nothing new, but they may reach new heights. Recent incidents this fall show that entire municipal or even national governments may be vulnerable to significant disruption from cybercriminals. "

Deepfake Phishing: A New Tool of Threat Actors

Source: https://www.cysecurity.news/2022/12/deepfake-phishing-new-tool-of-threat.html

From the Article: "Deepfake Phishing is an emerging attack vector that security experts should be concerned about because of the development of increasingly advanced AI, audio, and video technology as well as the abundance of user personal data that is

available on social media. "

Blackmailing MoneyMonger Malware Hides in Flutter Mobile Apps

Source: https://www.darkreading.com/vulnerabilities-threats/blackmailing-moneymonger-malware-hides-flutter-mobile-apps

From the Article: "Money-lending apps built using the Flutter software development kit hide a predatory spyware threat and highlight a growing trend of using personal data for blackmail."

DDoS Attack Platforms Shut Down in Global Law Enforcement Operation

Source: https://www.darkreading.com/attacks-breaches/ddos-attack-platforms-shut-down-in-global-law-enforcement-crackdown

From the Article: "Sweeping operation took down around 50 popular DDoS platforms, just one of which was used in 30M attacks, Europol says."

WatchGuard Threat Lab Report Finds Top Threat Arriving Exclusively Over Encrypted Connections

Source: https://www.darkreading.com/attacks-breaches/watchguard-threat-lab-report-finds-top-threat-arriving-exclusively-over-encrypted-connections

From the Article: "New research also analyzes the commoditization of adversary-in-the-middle attacks, JavaScript obfuscation in exploit kits, and a malware family with Gothic Panda ties."

NSA Slices Up 5G Mobile Security Risks

Source: https://www.darkreading.com/mobile/nsa-slices-up-5g-mobile-security-risks

From the Article: "The feds' mobile service provider guidance details cybersecurity threat vectors associated with 5G network slicing."

Link back to Table of Contents

Cybereason Warns Global Organizations Against Destructive Ransomware Attacks From Black Basta Gang

Source: https://www.darkreading.com/attacks-breaches/cybereason-warns-global-organizations-against-destructive-ransomware-attacks-from-black-basta-gang

From the Article: "The Royal Ransomware Group has emerged as a threat to companies in 2022 and they have carried out dozens of successful attacks on global companies. Cybereason suggests that companies raise their awareness of this potential pending threat."

CSAF Is the Future of Vulnerability Management

Source: https://www.darkreading.com/threat-intelligence/csaf-is-the-future-of-vulnerability-management

From the Article: "Version 2.0 of the Common Security Advisory Framework will enable organizations to automate vulnerability remediation."

Automated Cyber Campaign Creates Masses of Bogus Software Building Blocks

Source: https://www.darkreading.com/attacks-breaches/automated-cybercampaign-attacks-bogus-software-building-blocks

From the Article: "The proliferation of automated cyberattacks against npm, NuGet, and PyPI underscores the growing sophistication of threat actors and the threats to open source software supply chains."

Analysis Shows Attackers Favor PowerShell, File Obfuscation

Source: https://www.darkreading.com/edge-threat-monitor/analysis-shows-attackers-favor-powershell-file-obfuscation

From the Article: "Aiming to give threat hunters a list of popular attack tactics, a cybersecurity team analyzed collections of real-world threat data to find attackers' most popular techniques."

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Google Launches Scanner to Uncover Open Source Vulnerabilities

Source: https://www.darkreading.com/dr-tech/google-launches-scanner-to-uncover-open-source-vulnerabilities

From the Article: "OSV-Scanner generates a list of dependencies in a project and checks the OSV database for known vulnerabilities, Google says."

Citrix ADC, Gateway Users Race Against Hackers to Patch Critical Flaw

Source: https://www.darkreading.com/attacks-breaches/citrix-adc-gateway-users-race-against-hackers-patch-critical-flaw

From the Article: "Citrix issues a critical update as NSA warns that the APT5 threat group is actively trying to target ADC environments."

Accelerating Vulnerability Identification and Remediation

Source: https://www.darkreading.com/vulnerabilities-threats/accelerating-vulnerability-identification-and-remediation-

From the Article: "Software teams can now fix bugs faster with faster release cycles, but breach pressure is increasing. Using SBOM and automation will help better detect, prevent, and remediate security issues throughout the software development life cycle."

Security Flaw in Atlassian Products Affecting Multiple Companies

Source: https://www.darkreading.com/threat-intelligence/security-flaw-in-atlassian-products-affecting-multiple-companies

From the Article: "Jira, Confluence,Trello, and BitBucket affected."

Hackers Score Nearly $1M at Device-Focused Pwn2Own Contest

Source: https://www.darkreading.com/application-security/hackers-score-nearly-1-million-at-device-focused-pwn2own-contest

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

From the Article: "Offensive security researchers found 63 previously unreported vulnerabilities in printers, phones, and network-attached storage devices in the Zero Day Initiative's latest hackathon."

Rash of New Ransomware Variants Springs Up in the Wild

Source: https://www.darkreading.com/remote-workforce/rash-new-ransomware-variants-in-the-wild

From the Article: "Vohuk, ScareCrow, and AESRT add to the ransomware chaos that organizations have to contend with on a daily basis."

TPG reveals emails of 15,000 iiNet and Westnet customers exposed in hack

Source: https://www.theguardian.com/business/2022/dec/14/tpg-reveals-emails-of-15000-iinet-and-westnet-customers-exposed-in-hack

From the Article: "Telecommunications giant TPG has revealed an email-hosting service used by up to 15,000 iiNet and Westnet business customers has been breached, with the hacker looking for cryptocurrency and other financial information."

Top Cybersecurity Challenges for CISOs to Address in 2023

Source: https://www.fortinet.com/blog/ciso-collective/top-cybersecurity-challenges-for-cisos-to-address-in-2023

From the Article: "As 2022 comes to a close, read about some important threat landscape takeaways from the past 12 months. Learn about cybersecurity strategies and solutions that can best prepare CISOs for the cyber threats that could be coming in 2023."

Supply Chain Attack via New Malicious Python Package, "shaderz" (Part 2)

Source: https://www.fortinet.com/blog/threat-research/supply-chain-attack-via-new-malicious-python-package-shaderz-part-2

From the Article: "FortiGuard Labs recently discovered a 0-day attack in a PyPI package

called “shaderz.” "

Announcing OSV-Scanner: Vulnerability Scanner for Open Source

Source: https://security.googleblog.com/2022/12/announcing-osv-scanner-vulnerability.html

From the Article: "Today, we’re launching the OSV-Scanner, a free tool that gives open source developers easy access to vulnerability information relevant to their project."

Hive ransomware gang claims responsibility for attack on Intersport that left cash registers disabled

Source: https://www.bitdefender.com/blog/hotforsecurity/hive-ransomware-gang-claims-responsibility-for-attack-on-intersport-that-left-cash-registers-disabled/

From the Article: "Sports retail giant Intersport, which boasts some 6000 stores worldwide in 57 countries, has fallen victim to a ransomware attack which disabled checkouts in France during what should have been one of the busiest times of the year."

The State of Cybersecurity: Why Industry Experts Are Optimistic

Source: https://www.hackread.com/cybersecurity-industry-experts-optimistic/

From the Article: "2022 has been a tumultuous one for cybersecurity professionals. Breaches, hacks, and ransomware attacks have become commonplace in the news cycle, leaving many feeling vulnerable and uncertain about their digital safety."

Payment Giant Exposed 9 Million Credit Card Transaction Records

Source: https://www.hackread.com/exposed-credit-card-transaction-records/

From the Article: "The trove of sensitive data belonging to California-based Cornerstone Payment Systems was left exposed on a misconfigured server without any security authentication."

Link back to Table of Contents

Hackers Use SVG Files to Spread QBot Malware onto Windows Systems

Source: https://heimdalsecurity.com/blog/hackers-use-svg-files-to-spread-qbot-malware-onto-windows-systems/

From the Article: "A new technique for spreading QBot malware gained popularity among hackers – they are now distributing it through SVG files to perform HTML smuggling, which locally generates a malicious installer for Windows."

Social Blade Suffers Data Breach

Source: https://heimdalsecurity.com/blog/social-blade-suffers-data-breach/

From the Article: "On December 14th, Social Blade, a statistics website that allows its users to track statistics and measure growth across multiple Social Media platforms such as YouTube, Instagram, and Twitch, notified its clients about a potential data breach."

Mozilla Fixes Firefox Vulnerabilities That Could Have Lead to System Takeover

Source: https://heimdalsecurity.com/blog/mozilla-fixes-firefox-vulnerabilities-that-could-have-lead-to-system-takeover/

From the Article: "Multiple high-impact vulnerabilities affecting Thunderbird, Firefox ESR, and Firefox were fixed by updates from Mozilla. The bugs might have given arbitrary code execution if they were successfully exploited. "

New Attack Vector: 144k Phishing Packages Found on Open-source Repositories

Source: https://heimdalsecurity.com/blog/new-attack-vector-144k-phishing-packages-found-on-open-source-repositories/

From the Article: "Threat actors found a new attack vector spamming open-source ecosystem with packages that contain links to phishing campaigns. 144,294 phishing-related packages have been uploaded to open-source package repositories, like NPM, PyPi, and NuGet."

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

LockBit Ransomware 101: Here's What You Need to Know

Source: https://heimdalsecurity.com/blog/what-is-lockbit-ransomware/

From the Article: "LockBit ransomware is a malicious software designed for one thing: locking up the user's computer in exchange for a ransom. LockBit will automatically vet for targets and encrypt all your files that are accessible on your computer if you don't pay the ransom. "

The New Deepfake Regulations in China Raise Multiple Issues

Source: https://heimdalsecurity.com/blog/the-new-deepfake-regulations-in-china-raise-multiple-issues/

From the Article: "From January 20, 2023, new regulations regarding deepfake will be in place in China. Cyberspace Administration of China (CAC) declared that the purpose of these rules is to protect users from being impersonated."

Python and JavaScript Developers Exposed to Malware Infections

Source: https://heimdalsecurity.com/blog/python-and-javascript-developers-exposed-to-malware/

From the Article: "A sophisticated new malware campaign is targeting the Python Package Index and npm for both Python and JavaScript with typosquatted modules that deploy a ransomware strain. "

Vulnerabilities in Security Solutions Transform Them in Data Wipers

Source: https://heimdalsecurity.com/blog/vulnerabilities-in-security-solutions-transform-them-in-data-wipers/

From the Article: "Several Endpoint Detection and Response (EDR) and Antivirus (AV) products showed high-severity security vulnerabilities."

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Box Shield enhancements help reduce the risk of malicious attacks

Source: https://www.helpnetsecurity.com/2022/12/15/box-shield-enhancements/

From the Article: "Box has unveiled several enhancements to Box Shield, the company's flagship security solution for protecting content in the cloud."

Stellar Cyber and Deep Instinct integrate to help enterprises identify threats

Source: https://www.helpnetsecurity.com/2022/12/15/stellar-cyber-deep-instinct/

From the Article: "Stellar Cyber and Deep Instinct integration makes it easy for enterprise and MSSP customers using the Stellar Cyber Open XDR platform to deliver Deep Instinct's prevention capabilities across the entire attack surface."

OSV-Scanner: A free vulnerability scanner for open-source software

Source: https://www.helpnetsecurity.com/2022/12/14/vulnerabilities-open-source-dependencies/

From the Article: "After releasing the Open Source Vulnerabilities database (OSV.dev) in February, Google has launched the OSV-Scanner, a free command line vulnerability scanner that open source developers can use to check for vulnerabilities in their projects' dependencies."

3 major threat detection methods explained

Source: https://www.helpnetsecurity.com/2022/12/14/3-major-threat-detection-methods-explained/

From the Article: "The importance of threat detection cannot be overstated. A recent Verizon study revealed that the top discovery method (more than 50%) for breaches is in fact disclosure by the threat actor themselves after a successful compromise."

Searchlight Security Ransomware Search and Insights collates dark web data on ransomware groups

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Source: https://www.helpnetsecurity.com/2022/12/14/searchlight-security-ransomware-search-and-insights/

From the Article: "Searchlight Security launched Ransomware Search and Insights, a new strategic enhancement to its Cerberus platform."

Analyzing Australia's cyberthreat landscape, and what it means for the rest of the world

Source: https://www.helpnetsecurity.com/2022/12/13/australia-cyberattacks/

From the Article: "Australia has been the victim of damaging cyberattacks in the latter half of this year, with high-profile incidents impacting businesses across critical sectors such as telecoms, healthcare, and government. "

Palo Alto Networks Xpanse Active ASM evaluates cyber risks

Source: https://www.helpnetsecurity.com/2022/12/13/palo-alto-networks-xpanse-active-asm/

From the Article: "Palo Alto Networks has introduced a new Cortex capability: Xpanse Active Attack Surface Management, or Xpanse Active ASM. This helps security teams not just find but also fix their known and unknown internet-connected risks."

Iranian state-aligned threat actor targets new victims in cyberespionage and kinetic campaigns

Source: https://news.hitb.org/content/iranian-state-aligned-threat-actor-targets-new-victims-cyberespionage-and-kinetic-campaigns

From the Article: "TA435 is now employing more aggressive tactics, including the use of real email accounts, malware and confrontational lures to gain access to key accounts. The threat actor targets high-profile and high-security accounts for cyberespionage purposes."

Uber has been hacked yet again with code and employee data released online

Source: https://news.hitb.org/content/uber-has-been-hacked-yet-again-code-and-

Link back to Table of Contents

employee-data-released-online

From the Article: "Uber Technologies Inc. has suffered yet another data breach, with a hacker sharing the stolen data on BreachForums, the successor forum for the now-shuttered RaidForums."

Effective, fast, and unrecoverable: Wiper malware is popping up everywhere

Source: https://news.hitb.org/content/effective-fast-and-unrecoverable-wiper-malware-popping-everywhere

From the Article: "Over the past year, a flurry of destructive wiper malware from no fewer than nine families has appeared. In the past week, researchers cataloged at least two more, both exhibiting advanced codebases designed to inflict maximum damage."

Iran-sponsored group using GitHub to deploy custom malware

Source: https://news.hitb.org/content/iran-sponsored-group-using-github-deploy-custom-malware

From the Article: "The Secureworks Counter Threat Unit (CTU) has uncovered a subgroup of Iranian Cobalt Mirage using GitHub to store and deploy malware."

US Senate clears bipartisan bill that boosts national security by preparing for quantum cybersecurity risks

Source: https://industrialcyber.co/vulnerabilities/us-senate-clears-bipartisan-bill-that-boosts-national-security-by-preparing-for-quantum-cybersecurity-risks/

From the Article: "The U.S. Senate recently passed a bipartisan legislative bill that works on strengthening national security by preparing the federal government's defenses against quantum computing-enabled data breaches."

Microsoft report finds attackers use multiple tactics, approaches to target OT, as critical infrastructure risks rise

Source: https://industrialcyber.co/it-ot-collaboration/microsoft-report-finds-attackers-use-

multiple-tactics-approaches-to-target-ot-as-critical-infrastructure-risks-rise/

From the Article: "A new Microsoft report provided new insights on wider risks that converging IT, Internet of Things (IoT), and operational technology (OT) systems pose to critical infrastructure."

FCC proposes requirements for emergency alert system participants to report cybersecurity incidents

Source: https://industrialcyber.co/regulation-standards-and-compliance/fcc-proposes-requirements-for-emergency-alert-system-participants-to-report-cybersecurity-incidents/

From the Article: "The Federal Communications Commission (FCC) published Wednesday a notice in the Federal Register proposing requirements for emergency alert system (EAS) participants to report compromises of their equipment, communications systems, and services to the commission. "

Platforms Flooded with 144,000 Phishing Packages

Source: https://www.infosecurity-magazine.com/news/platforms-flooded-144000-phishing/

From the Article: "A phishing group has uploaded over 144,000 malicious open source packages to three open source repositories, in a major new automated campaign, according to Checkmarx."

Over 85% of Attacks Hide in Encrypted Channels

Source: https://www.infosecurity-magazine.com/news/over-85-attacks-hide-encrypted/

From the Article: "Zscaler reveals 20% increase in malicious use of encryption."

Loan Scam Campaign 'MoneyMonger' Exploits Flutter to Hide Malware

Source: https://www.infosecurity-magazine.com/news/loan-scam-campaign-moneymonger/

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

From the Article: "Zimperium said the code was part of an existing campaign previously discovered by K7 Security Labs."

AgentTesla Remains Most Prolific Malware in November, Emotet and Qbot Grow

Source: https://www.infosecurity-magazine.com/news/agenttesla-top-november-malware/

From the Article: "These are some of the key findings from the latest Check Point Research Most Wanted report."

Uber Hit By New Data Breach After Attack on Third-Party Vendor

Source: https://www.infosecurity-magazine.com/news/uber-hit-by-new-data-breach/

From the Article: "Company information was stolen from third-party vendor Teqtivity and posted on a dark web forum."

The state of Identity Security: Widespread attacks, wasted investment and identity sprawl

Source: https://www.itsecurityguru.org/2022/12/15/the-state-of-identity-security-widespread-attacks-wasted-investment-and-identity-spawl/

From the Article: "Surveying over 1,000 IT security professionals, the results showed that 96 percent of companies report using multiple identity management tools, with 41 percent deploying at least 25 different systems to manage access rights."

Command injection vulnerability in SHARP Multifunctional Products (MFP)

Source: https://jvn.jp/en/vu/JVNVU96195138/

From the Article: "SHARP Multifunctional Products (MFP) contain a command injection vulnerability."

Multiple vulnerabilities in DENSHI NYUSATSU CORE SYSTEM

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Source: https://jvn.jp/en/jp/JVN96321933/

From the Article: "DENSHI NYUSATSU CORE SYSTEM provided by Japan Construction Information Center contains multiple vulnerabilities."

Redmine vulnerable to cross-site scripting

Source: https://jvn.jp/en/jp/JVN60211811/

From the Article: "Redmine contains a cross-site scripting vulnerability."

E-mail threat trends in 2022 | Kaspersky official blog

Source: https://www.kaspersky.com/blog/email-threats-in-2022/46582/

From the Article: "The pandemic completely reshaped the e-mail threat landscape. The mass shift over to remote working and the inevitable transfer of most communications to the online format has stimulated a rise in both phishing and BEC attacks. "

Microsoft Digital Certificates Have Once Again Been Abused To Sign Malware

Source: https://arstechnica.com/information-technology/2022/12/microsoft-digital-certificates-have-once-again-been-abused-to-sign-malware/

From the Article: "Microsoft has once again been caught allowing its legitimate digital certificates to sign malware in the wild, a lapse that allows the malicious files to pass strict security checks designed to prevent them from running on the Windows operating system."

Play ransomware attacks city of Antwerp

Source: https://www.malwarebytes.com/blog/news/2022/12/play-ransomware-attacks-government-agencies-and-their-providers

From the Article: "The city of Antwerp’s digital systems have come to a grinding halt. The Flemish government under which Antwerp resides has confirmed that this is the result of a ransomware attack."

Link back to Table of Contents

Silence is golden partner for Truebot and Clop ransomware

Source: https://www.malwarebytes.com/blog/news/2022/12/silence-is-golden-partner-for-truebot-and-clop-ransomware

From the Article: "A recent rise in the number of Truebot infections has been attributed to a threat actor known as the Silence Group. The Silence Group is an initial access broker (IAB) that frequently changes tools and tactics to stay on top of the game."

MCCrash: Cross-platform DDoS botnet targets private Minecraft servers

Source: https://www.microsoft.com/en-us/security/blog/2022/12/15/mccrash-cross-platform-ddos-botnet-targets-private-minecraft-servers/

From the Article: "Malware operations continue to rapidly evolve as threat actors add new capabilities to existing botnets, increasingly targeting and recruiting new types of devices."

Cyber Signals: Risks to critical infrastructure on the rise

Source: https://www.microsoft.com/en-us/security/blog/2022/12/14/cyber-signals-risks-to-critical-infrastructure-on-the-rise/

From the Article: "Today, the third edition of Cyber Signals was released spotlighting security trends and insights gathered from Microsoft's 43 trillion daily security signals and 8,500 security experts."

Elon Musk Takes Legal Action To Bully Student That Tracks His Plane With PUBLIC Data

Source: https://gizmodo.com/elon-musk-legal-action-elonjet-jack-sweeney-1849897068

From the Article: "Twitter CEO and owner Elon Musk is taking legal action against Jack Sweeney, the University of Central Florida student who tracks his private plane and publishes his flight information on social media under the @ElonJet banner."

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Google Launches New Tool To Identify Open Source Vulnerabilities

Source: https://www.scmagazine.com/analysis/vulnerability-management/google-launches-new-tool-to-identify-open-source-vulnerabilities

From the Article: "The Go-based tool — called OSV-Scanner — provides an automated capability to match a developer's code and dependencies against lists of known vulnerabilities and deliver instant feedback if patches or updates are needed. "

Iran-Linked Charming Kitten Espionage Gang Phishing Politicians

Source:
https://www.theregister.com/2022/12/15/charming_kitten_ta453_expands_targets/

From the Article: "An Iranian cyber espionage gang with ties to the Islamic Revolutionary Guard Corps has learned new methods and phishing techniques, and aimed them at a wider set of targets – including politicians, government officials, critical infrastructure and medical researchers – according to email security vendor Proofpoint."

NSA Warns Chinese Hackers Are Exploiting Citrix Gear

Source: https://www.scmagazine.com/analysis/remote-access/chinese-hackers-exploiting-bug-in-citrix-adc-gateway-products-nsa-warns

From the Article: "A newly disclosed vulnerability in Citrix application delivery controllers and its Gateway remote access solution allows an unauthenticated attacker to execute arbitrary code, and follow-up guidance from U.S. national security officials indicate that a Chinese-linked advanced persistent threat group has already made use of it. "

Teqtivity Pwn Results In Uber Staff Info Leak

Source: https://www.theregister.com/2022/12/13/uber_data_breach_teqtivity/

From the Article: "Uber, which has suffered a few data thefts in its time, is this week dealing with the fallout from yet another – this time from one of its technology suppliers."

This Evasive New Cyberattack Can Bypass Air-Gapped Systems To Steal Data From The

Link back to Table of Contents

Most Sensitive Networks

Source: https://www.zdnet.com/article/this-evasive-new-cyberattack-can-bypass-air-gapped-systems-to-steal-data-from-the-most-sensitive-networks/

From the Article: "Cybersecurity researchers have demonstrated a novel method of cyberattack that could allow malicious hackers to steal information from some of the most well-protected computers."

Pwn2Own Pays Out Almost $1m To Ethical Hackers

Source: https://www.theregister.com/2022/12/13/pwn2own_wraps/

From the Article: "Pwn2Own paid out almost $1 million to bug hunters at last week's consumer product hacking event in Toronto, but the prize money wasn't big enough attract attempts at cracking the iPhone or Google Pixel because miscreants can score far more from less wholesome sources."

Find and Fix Your Unknown Risk With Active Attack Surface Management

Source: https://www.paloaltonetworks.com/blog/2022/12/active-attack-surface-management-with-cortex-xpanse/

From the Article: "Organizations are evolving to meet the demands of cloud and hybrid work, but this acceleration leads to an expansion in their unmanaged attack surface. Certain industries, including healthcare and insurance, saw a 20-25% increase in new risks on their unmanaged attack surface every month, according to the 2022 Attack Surface Threat Report. No industry showed a reduction in attack surface risks."

Sirius XM vulnerability allowed hackers to unlock cars, start engines

Source: https://www.pandasecurity.com/en/mediacenter/security/sirius-xm-vulnerability/

From the Article: "Bug bounty hunter Sam Curry discovered a vulnerability in the SiriusXM Connected Vehicle Services telematics platform that allowed him to remotely perform unauthorized tasks in smart cars such as unlocking, starting the engine, and even honking any remotely connected Honda, Nissan, Infiniti, and Acura vehicles."

Link back to Table of Contents

Iran-linked cyberspies expand targeting to medical researchers, travel agencies

Source: https://www.proofpoint.com/us/newsroom/news/iran-linked-cyberspies-expand-targeting-medical-researchers-travel-agencies

From the Article: "A cyberespionage group aligned with Iran's Islamic Revolutionary Guard Corps (IRGC) has been observed attacking new targets over the last two years, including medical researchers, an aerospace engineer and even a Florida-based realtor."

Major Canadian grocery chain says cyberattack cost $25 million | CBC News

Source: https://www.cbc.ca/news/canada/nova-scotia/sobeys-cyber-attack-25-million-1.6686838

From the Article: "The parent company of the Sobeys grocery store chain says a cyberattack last month will cost $25 million."

Ransomware groups are on the prowl: Could you be their next target? | Fox News

Source: https://www.foxnews.com/tech/ransomware-groups-prowl-next-target

From the Article: "If malware and viruses weren't enough to worry about, everyday people continue to be subjected to ransomware, software designed to block access to networks, systems and files, often in the form of an email or contaminated app, until a sum of money, usually around $300 or so is paid."

Interagency Task Force Reviews Actions to Reduce Impact of Ransomware Incidents in 2nd Meeting

Source: https://executivegov.com/2022/12/interagency-task-force-reviews-actions-to-reduce-impact-of-ransomware-incidents/

From the Article: "The Joint Ransomware Task Force held Wednesday its second meeting and assessed measures and efforts carried out by working groups to address the impact and prevalence of ransomware incidents."

Link back to Table of Contents

How would a data leak affect your organisation? - New Statesman

Source: https://www.newstatesman.com/spotlight/cybersecurity/2022/12/data-leak-cybersecurity-ransomware-stolen-information

From the Article: "Ransomware is a bigger problem now than it has ever been. Generally, in the past, the modus operandi of criminals using ransomware involved them getting into an organisation's computer network, encrypting its files, then sending their victims a message saying something like, "We've encrypted your stuff – pay us a ransom and we'll give it back.""

Think of cyber insurance as a strategic business decision | SC Media

Source: https://www.scmagazine.com/perspective/ransomware/think-of-cyber-insurance-as-a-strategic-business-decision

From the Article: "The cyber insurance market has been valued at roughly $12 billion and could triple to more than $29 billion by 2027. Cyber insurance, unlike automobile and some other forms of insurance, has not yet been made mandatory, but it's set to become indispensable to companies involved in merger or partnership negotiations, or in raising money from investors."

Action against booter services. Anti-ransomware task force. AIIMS incident update. The ...

Source: https://thecyberwire.com/newsletters/daily-briefing/11/239

From the Article: "Alleged booters collared, their sites disabled. Progress report on US anti-ransomware efforts. "

Play ransomware gang targets Antwerp's IT solutions provider, disrupts municipal ... - teiss

Source: https://www.teiss.co.uk/news/play-ransomware-gang-targets-antwerps-it-solutions-provider-disrupts-municipal-healthcare-services-11380

From the Article: "The Play ransomware gang has claimed responsibility for the cyber attack on Digipolis."

Link back to Table of Contents

Direct Means Proximate? Oregon District Court Holds Ransomware Payment Is a Direct Loss

Source: https://www.jdsupra.com/legalnews/direct-means-proximate-oregon-district-9427502/

From the Article: "In yet another troubling decision to the crime insurance industry, on Dec. 6, a federal district court, applying Oregon law, found coverage for a ransomware payment under a Computer Fraud insuring agreement."

Ransomware Protection Market Size: 2022, Development Perspectives, Business Trends ...

Source: https://www.digitaljournal.com/pr/ransomware-protection-market-size-2022-development-perspectives-business-trends-and-research-forecasts-to-2030-microsoft-corporation-sophos-ltd-trend-micro-incorporated

From the Article: "The Ransomware Protection Market Research Report offers extensive information on the following topics – Industry size, share, growth, segmentation, manufacturers and progress, main trends, market drivers, challenges, standardization, deployment models, opportunities, strategies, future road maps, and Annual forecast till 2030 provides a complete study of the global Ransomware Protection Market."

Ransomware Guide 2022: Identifying Real, Fake Attacks, How to Avoid It, and More!

Source: https://www.techtimes.com/articles/284960/20221215/ransomware-guide-2022-identifying-real-fake-attacks-avoid-more.htm

From the Article: "Ransomware attacks are still rampant. This is why it is important to know the cybersecurity measures that can protect you from scams and other malicious campaigns."

Check Point classifies Azov as wiper, not ransomware - TechTarget

Source: https://www.techtarget.com/searchsecurity/news/252528410/Check-Point-classifies-Azov-as-wiper-not-ransomware

Link back to Table of Contents

From the Article: "Check Point Software Technologies researchers analyzed thousands of Azov samples uploaded to VirusTotal and discovered the malware was crafted with more advanced techniques than initially thought."

How to deal with cyberattacks this holiday season - Tripwire

Source: https://www.tripwire.com/state-of-security/how-deal-cyberattacks-holiday-season

From the Article: "The holiday season has arrived, and cyberattacks are expected to increase with the upcoming celebratory events. According to The Retail & Hospitality Information Sharing and Analysis Center (RH-ISAC) 2022 Holiday Season Threat Trends and summary report, ransomware and phishing attacks are expected to increase in retail."

How Ransomware Puts Your SAAS Data at Risk – And How To Protect It - CPO Magazine

Source: https://www.cpomagazine.com/cyber-security/how-ransomware-puts-your-saas-data-at-risk-and-how-to-protect-it/

From the Article: "The cyber threat landscape is constantly evolving, and ransomware poses an increasing risk to businesses and their critical data."

Trend Micro Urges Security Teams to Prepare for the Next Era of Ransomware

Source: https://www.marketscreener.com/quote/stock/TREND-MICRO-INCORPORATED-120787643/news/Trend-Micro-Urges-Security-Teams-to-Prepare-for-the-Next-Era-of-Ransomware-42555516/

From the Article: "Global cybersecurity leader Trend Micro published a new report today warning that the ransomware industry could be on the verge of a revolution that sees actors expand into other areas of cybercrime or partner with hostile governments and organized crime groups."

Ransomware Business Models: Future Pivots and Trends - Trend Micro

Link back to Table of Contents

Source: https://www.trendmicro.com/en_us/research/22/l/ransomware-business-models-future-trends.html

From the Article: "Ransomware groups and their business models are expected to change from what and how we know it to date. In this blog entry, we summarize from some of our insights the triggers that spark the small changes in the short term ("evolutions") and the bigger deviations ("revolutions") they can redirect their criminal enterprises to in the long run."

The Professionalization of Ransomware: What You Need to Know - InformationWeek

Source: https://www.informationweek.com/security-and-risk-strategy/the-professionalization-of-ransomware-what-you-need-to-know

From the Article: "The rise of ransomware-as-a-service (RaaS) is just one marker in the emergence of a more organized and professional class of ransomware gangs focused on new ways of monetizing ransomware beyond encryption, including double and triple extortion."

Abertay cyberQuarter's founding partners include ransomware victim - FutureScot

Source: https://futurescot.com/abertay-cyberquarters-founding-partners-include-ransomware-victim/

From the Article: "Weir Group, hit last year by a cyberattack, will be one of 11 partner organisations supporting Scotland's new hub for cybersecurity research, development and economic growth."

Interagency task force digs into measurement capabilities for ransomware trends

Source: https://insidecybersecurity.com/daily-news/interagency-task-force-digs-measurement-capabilities-ransomware-trends-partnership

From the Article: "The Joint Ransomware Task Force led by CISA and the FBI is looking into how to use data and other metrics from information collected by the government on ransomware to determine trends and inform federal activities, according to a CISA meeting readout."

Link back to Table of Contents

How the NSA and private sector are working together on cybersecurity - Marketplace.org

Source: https://www.marketplace.org/shows/marketplace-tech/nsa-private-sector-cybersecurity/

From the Article: "A government agency known for keeping its secrets has been attempting to be a bit more open when it comes to cybersecurity."

G7 Cyber Expert Group releases reports on ransomware and third-party risk - Lexology

Source: https://www.lexology.com/library/detail.aspx?g=750482a1-8fb0-4a98-bc20-6597bda0c5fa

From the Article: "On December 8, the G7 Cyber Expert Group (CEG) – co-chaired by the Bank of England and the U.S. Treasury Department's Office of Cybersecurity and Critical Infrastructure – released two reports addressing ransomware and third-party risk in the financial sector."

The Future of Ransomware - Noticias de seguridad - Trend Micro ES

Source: https://www.trendmicro.com/vinfo/es/security/news/cybercrime-and-digital-threats/the-future-of-ransomware

From the Article: "In response to these counteroffensives, ransomware groups have shown that specific triggers cause them to adjust their criminal business models."

Breaking news: Ottawa-area IT firm says it has fully recovered from ransomware attack

Source: https://www.itworldcanada.com/article/breaking-news-ottawa-area-it-firm-says-it-has-fully-recovered-from-ransomware-attack/518084

From the Article: "Marc Villeneuve, owner of 2NetworkIT, credits having a resilient backup strategy for being able to bypass the issue of 11 encrypted servers and restore most data for the company's 30 customers after 48 hours."

Link back to Table of Contents

Cuba ransomware - SystemTek

Source: https://www.systemtek.co.uk/2022/12/cuba-ransomware/

From the Article: "Demanded 145 million U.S. Dollars (USD) and received 60 million USD in ransom payments."

Readout of Second Joint Ransomware Task Force Meeting - CISA

Source: https://www.cisa.gov/news/2022/12/14/readout-second-joint-ransomware-task-force-meeting

From the Article: "The Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) co-chaired the second meeting today of the Joint Ransomware Task Force (JRTF), an inter-agency body established by Congress to unify and strengthen efforts against the ongoing threat of ransomware. The first JRTF meeting was held in September 2022. "

The Dark Web is Getting Darker - Ransomware Thrives on Illegal Markets

Source: https://www.bleepingcomputer.com/news/security/the-dark-web-is-getting-darker-ransomware-thrives-on-illegal-markets/

From the Article: "In April 2022, the U.S. Treasury sanctioned the Russia-based Hydra Market. Hydra, the world's largest dark web market, provided malicious cybercrime and cryptocurrency exchange services to global threat actors. The U.S. and Germany shut Hydra down around the same time."

US finds its 'center of gravity' in the fight against ransomware

Source: https://therecord.media/us-finds-its-center-of-gravity-in-the-fight-against-ransomware/

From the Article: "Momentum is building around a recently created Biden administration task force meant to unite the federal government in a common purpose: stem the tide of ransomware attacks that has flooded the country."

Link back to Table of Contents

HC3 warns healthcare organizations of BlackCat ransomware variant

Source: https://www.beckershospitalreview.com/cybersecurity/hc3-warns-healthcare-organizations-of-blackcat-ransomware-variant.html

From the Article: "The Health Sector Cybersecurity Coordination Center, or HC3, is warning healthcare organizations to be on the lookout for the BlackCat ransomware variant."

Ohio city suffers ransomware attack. Investment firm CEO sues IRS for leaking tax ...

Source: https://thecyberwire.com/newsletters/privacy-briefing/4/238

From the Article: "More on LockBit ransomware attack on the California Department of Finance. Uber data takes another ride to the dark web."

Increased risk for detrimental damage caused by ransomware gangs - SecurityBrief Asia

Source: https://securitybrief.com.au/story/increased-risk-for-detrimental-damage-caused-by-ransomware-gangs

From the Article: "Additionally, Avast researchers foresee optimisation of social engineering used in scam attacks, taking advantage of economic hardships and energy crisis fears. The experts also expect increased malicious activity overall, as open-source malware becomes more accessible, and cybergangs recruit hacktivists to join their causes."

Searchlight Security Offers MSSPs Ransomware Dark Web Tracking Tool - MSSP Alert

Source: https://www.msspalert.com/cybersecurity-services-and-products/threat-intelligence/searchlight-security-offers-mssps-ransomware-dark-web-tracking-tool/

From the Article: "The Ransomware Search and Insights enhancement is intended to help managed security service providers (MSSPs), organizations and law enforcement to investigate, track, and gather intelligence on live ransomware activity."

Delhi AIIMS ransomware attack carried out by hackers from China, Hong Kong: Report

Link back to Table of Contents

Source: https://www.wionews.com/india-news/attack-on-aiims-delhi-server-carried-out-by-chinese-hackers-report-543044

From the Article: "The ransomware attack on the servers of the All India Institute of Medical Sciences (AIIMS), Delhi was carried out by Chinese hackers, news agency ANI reported on Wednesday citing a government source."

Microsoft-Signed Malicious Driver Used in Pre-Ransomware Intrusions - Duo Security

Source: https://duo.com/decipher/microsoft-signed-malicious-driver-used-in-pre-ransomware-intrusions

From the Article: "Researchers from three separate organizations recently discovered that threat actors were deploying a malicious Windows driver that had been signed by a legitimate Microsoft developer certificate as part of post-exploitation activity, sometimes leading up to ransomware deployment."

CommonSpirit Health reports more than 600k people had data at risk in ransomware attack

Source: https://www.kitsapsun.com/story/news/local/2022/12/14/commonspirit-health-data-cyberattack-st-michael-medical-center-silverdale-washignton/69722608007/

From the Article: "CommonSpirit Health reported to the federal government earlier this month that more than 600,000 individuals had their information exposed in a ransomware attack that disrupted operations at St. Michael Medical Center and other health care facilities in October."

Ransomware Threats Are Growing. How Can Boards Protect Mission-Critical Assets?

Source: https://www.corporatecomplianceinsights.com/risk-ransomware-board/

From the Article: "A ransomware attack is every organization’s nightmare. Even with concerted efforts to understand and manage the threat, the uncertainty created by must-read headlines of the chaos that high-profile attacks engender is troubling to senior executives and directors alike. Smart leaders know a strategic response is needed."

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Zoom Program: The Ransomware Hunting Team | Danvers, MA Patch

Source: https://patch.com/massachusetts/danvers/calendar/event/20230125/9a97f760-e996-4805-86e0-31c5cfd4623e/zoom-program-the-ransomware-hunting-team

From the Article: "Join authors Pulitzer Prize finalist Renee Dudley and local Pulitzer Prize winner Daniel Golden as they discuss their latest book, The Ransomware Hunting Team."

Combating Ransomware Attacks: Which Strategies Hold Promise? - BankInfoSecurity

Source: https://www.bankinfosecurity.com/interviews/combating-ransomware-attacks-which-strategies-hold-promise-i-5195

From the Article: "Hi, I'm Mathew Schwartz with Information Security Media Group and I'm sitting down at Black Hat Europe with Jen Ellis, a cybersecurity - some might say veteran - but someone with deep experience in the field. Jen, great to have you here today."

How the Federal Government Can Improve Its Response to Ransomware Attacks

Source: https://fedtechmagazine.com/article/2022/12/how-federal-government-can-improve-its-response-ransomware-attacks

From the Article: "While the federal government is not the primary target of ransomware attacks, it plays a large role in helping those who have been attacked recover. It also provides advice on how enterprises can protect themselves against such attacks."

HHS Warns Healthcare Sector of LockBit 3.0, BlackCat Ransomware - HealthITSecurity

Source: https://healthitsecurity.com/news/hhs-warns-healthcare-sector-of-lockbit-3.0-blackcat-ransomware

From the Article: "LockBit 3.0 and BlackCat ransomware have been known to target healthcare organizations with highly sophisticated tactics."

What Is BlackCat Ransomware and How Can You Prevent It? - MakeUseOf

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Source: https://www.makeuseof.com/what-is-blackcat-ransomware/

From the Article: "Unlike other cyberattacks, BlackCat ransomware operates on a powerful programming language that is hard to decode. What exactly is BlackCat ransomware and what are your chances of preventing it?"

Feds warn healthcare sector about LockBit 3.0 ransomware threat

Source: https://www.beckershospitalreview.com/cybersecurity/feds-warn-healthcare-sector-about-lockbit-3-0-ransomware-threat.html

From the Article: "HHS issued a brief Dec. 12 warning healthcare organizations about the cybersecurity risks associated with ransomware group LockBit 3.0."

How Criminals Extort Healthcare Victims With Ransomware

Source: https://www.bankinfosecurity.com/how-criminals-extort-healthcare-victims-ransomware-a-20708

From the Article: "Ransomware operations have become expert at finding ways to make a victim pay, and healthcare organizations are no exception. But experts say there are multiple steps healthcare sector entities in particular can take to better protect themselves and ensure that in the event of an attack, they can quickly restore systems and never have to consider paying a ransom."

Royal Ransomware Puts Novel Spin on Encryption Tactics - Dark Reading

Source: https://www.darkreading.com/attacks-breaches/royal-ransomware-novel-spin-encryption-tactics

From the Article: "The Royal ransomware gang has quickly risen to the top of the ransomware food chain, demonstrating sophisticated tactics — including partial and rapid encryption — that researchers believe may reflect the years of experience its members honed as leaders of the now-defunct Conti Group."

Cyber Security Today, Dec. 14, 2022 – A botnet tries to brute-force WordPress ... - IT World Canada

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Source: https://www.itworldcanada.com/article/cyber-security-today-dec-14-2022-a-botnet-tries-to-brute-force-wordpress-sites-a-warning-to-atlassian-admins-and-new-ransomware-tactics/517922

From the Article: "I'll start with a warning to WordPress and OpenCart website administrators: A new botnet has been discovered that tries to brute-force its way into poorly-protected websites."

Cybereason warns of rapid increase in Royal ransomware | TechTarget

Source: https://www.techtarget.com/searchsecurity/news/252528326/Cybereason-warns-of-rapid-increase-in-Royal-ransomware

From the Article: "Royal ransomware is on the rise as operators have embraced partial encryption to evade detection, a newer technique that's becoming a trend among other ransomware gangs."

Responding to ransomware in the public cloud - Rubrik - ITWeb

Source: https://www.itweb.co.za/webinar/responding-to-ransomware-in-the-public-cloud/

From the Article: "Rubrik, in partnership with ITWeb, invites you to this event to learn how to weigh up the risks vs benefits of the public cloud for data and applications. You will discover how local organisations unwittingly increase their risk profiles in the cloud, and common assumptions that could put their data at risk."

Ransomware is coming for corporate back-up servers - Channel Asia

Source: https://www.networkworld.com/article/3682659/ransomware-it-s-coming-for-your-backup-servers.html

From the Article: "Back-up and recovery systems are at risk for two types of ransomware attacks: encryption and exfiltration – and most on-premises back-up servers are wide open to both."

Nubeva Announces Another Successful Ransomware Decryption - EIN News

Source: https://www.einnews.com/pr_news/606071842/nubeva-announces-another-

Link back to Table of Contents

successful-ransomware-decryption

From the Article: "Nubeva's patented Ransomware Reversal technology captures ransomware encryption materials at the moment of attack, enabling victim organizations to decrypt locked files without paying the ransom."

AIIMS ransomware attack: Probe reveals 'China-link'; hacker threatened to sell data on dark web

Source: https://economictimes.indiatimes.com/news/india/aiims-ransomware-attack-probe-reveals-china-link-hacker-threatened-to-sell-data-on-dark-web/videoshow/96223238.cms

From the Article: "Probe reveals 'China-link' in the AIIMS Delhi server hacking case."

AIIMS Ransomware Attack Originated from China, Data on 5 Hacked Servers Retrieved: Sources

Source: https://www.news18.com/news/india/aiims-ransomware-attack-originated-from-china-data-on-5-hacked-servers-retrieved-sources-6614587.html

From the Article: "Trouble began on November 23 when the servers went down, affecting the outpatient department (OPD) and sample collection services."

Cybersecurity top of mind for Alamo Regional Security Operation Center facility - KSAT.com

Source: https://www.ksat.com/news/local/2022/12/14/cybersecurity-top-of-mind-for-alamo-regional-security-operation-center-facility/

From the Article: "Cyber security is top of mind more than a week after San Antonio-based company Rackspace fell victim to ransomware."

Catalogic protects Azure and GCP VMs against ransomware - Blocks and Files

Source: https://blocksandfiles.com/2022/12/14/leftward-stretching-catalogic-extends-ransomware-defences-and-protects-azure-and-gcp-vms/

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

From the Article: "Catalogic has its Cloud Backup-as-a-Service offering for containerized applications on-premises or in the cloud, and its DPX suite for bare metal and virtualized workloads running on-premises."

Why Educational Institutions are Prone to Ransomware Attacks (and What They Can Do to ...

Source: https://thejournal.com/articles/2022/12/13/why-educational-institutions-are-prone-to-ransomware-attacks.aspx?m=1

From the Article: "Ransomware is the most significant information security threat in the education sector, and K–12 schools and colleges and universities are both targets. For example, Los Angeles Unified School District, the second largest district in the U.S. with more than 1,000 schools and 600,000 students, was recently hit by a ransomware attack, disrupting access to its IT systems. "

Flashpoint finds Australia the sixth most targeted country for ransomware

Source: https://securitybrief.com.au/story/flashpoint-finds-australia-the-sixth-most-targeted-country-for-ransomware

From the Article: "The report also found that LockBit was leading the charge when it came to ransomware groups, and the top industries targeted were professional services (20.7%), internet and software services (18.5%), and construction and engineering (14.1%). Overall, these sectors accounted for more than 50% of targeted malicious activity."

BlackCat, LockBit 3.0 ransomware target healthcare with customizable tactics, triple extortion

Source: https://www.scmagazine.com/analysis/ransomware/blackcat-lockbit-3-0-ransomware-target-healthcare-with-customizable-tactics-triple-extortion

From the Article: "Healthcare cybersecurity leaders are being urged to review the IOCs and the recommended proactive measures for defending against BlackCat and LockBit 3.0 ransomware variants given the continued targeting of healthcare environments."

Link back to Table of Contents

LockBit 3.0 Ransomware Threatens Health Sector, Feds Warn - BankInfoSecurity

Source: https://www.bankinfosecurity.com/lockbit-30-ransomware-threatens-health-sector-feds-warn-a-20700

From the Article: "U.S. federal authorities are warning healthcare and public health sector organizations of attacks involving LockBit 3.0 ransomware, which includes features of other ransomware variants along with the threat of triple-extortion demands."

California hospital breach exposed patients' Social Security numbers, medical info

Source: https://therecord.media/california-hospital-breach-exposed-patients-social-security-numbers-medical-info/

From the Article: "A hospital in California's Riverside County has reported a data breach to its patients including sensitive information like Social Security numbers and the details of medical care following an incident in the fall. "

PyPI and NPM code repositories targeted in ongoing ransomware attack - Tech Monitor

Source: https://techmonitor.ai/technology/cybersecurity/pypi-ransomware-python-npm

From the Article: "Developers using PyPI and NPM code repositories are being targeted with ransomware. Attackers are deploying the malware using fake modules and a technique called typosquatting, that lures victims into downloading a fake and malicious piece of code. "

Irish Healthcare Ransomware Hack Cost Over 80 Million Euros

Source: https://www.bankinfosecurity.com/irish-healthcare-ransomware-hack-cost-over-80-million-euros-a-20699

From the Article: "A ransomware attack on the Irish healthcare system in 2021 has caused 80 million euros in damages and counting as the government continues to notify victims of the incident that their personal information was illegally accessed and copied."

Travis Central Appraisal District back to normal operations after ransomware attack -

Link back to Table of Contents

KVUE

Source: https://www.kvue.com/video/news/local/travis-county-appraisal-district-ransomware-attack/269-268942d3-6dd1-489b-b399-bd01cb552f95

From the Article: "The Travis Central Appraisal District's phone service and online chat are up and running again after a ransomware attack a week ago."

Ransomware hits school computer system in Guntur - The Hindu

Source: https://www.thehindu.com/news/national/andhra-pradesh/ransomware-hits-school-computer-system-in-guntur/article66259969.ece

From the Article: "In probably a first of its kind incident, Ransomware hit a well-known school in Guntur in Andhra Pradesh. The cyber wing of the Guntur district police have launched an investigation and analysing the software."

Play Ransomware gang breaches Antwerp, 557GB of data stolen - Candid.Technology

Source: https://candid.technology/play-ransomware-antwerp-557gb-data/

From the Article: "The Belgian city of Antwerp has been attacked by the Play ransomware gang. The threat actor breached Digipolis — the IT company handling the city's IT systems which disrupted email, phone and internet services. The disruption is still active at the time of writing."

Effective, fast, and unrecoverable: Wiper malware is popping up everywhere | Ars Technica

Source: https://arstechnica.com/information-technology/2022/12/effective-fast-and-unrecoverable-wiper-malware-is-popping-up-everywhere/

From the Article: "Over the past year, a flurry of destructive wiper malware from no fewer than nine families has appeared. In the past week, researchers cataloged at least two more, both exhibiting advanced codebases designed to inflict maximum damage."

Open Source Software Are Targeted By A Ransomware Campaign

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Source: https://www.opensourceforu.com/2022/12/open-source-software-are-targeted-by-a-ransomware-campaign-with-a-carefully-disguised-payload/

From the Article: "The campaign, which includes embedded malware, targets the well-known “requests” package on Pypi and the “discord.js” package on NPM, according to a blog post by Checkmarx researchers. When the ransomware is run, it encrypts the victim’s computer data and demands $100 in cryptocurrency to decrypt them."

Malware Strains Targeting Python and JavaScript Developers Through Official Repositories

Source: https://thehackernews.com/2022/12/malware-strains-targeting-python-and.html

From the Article: "An active malware campaign is targeting the Python Package Index (PyPI) and npm repositories for Python and JavaScript with typosquatted and fake modules that deploy a ransomware strain, marking the latest security issue to affect software supply chains."

Growing risk of cyber-attacks come in the form of Ransomware and Malware

Source: https://www.businessleader.co.uk/growing-risk-of-cyber-attacks-come-in-the-form-of-ransomware-and-malware/

From the Article: "89% of SMB leaders are increasingly concerned by the growing risk of cyber-attacks in the form of Ransomware and Malware, according to a new survey by DataSolutions Group, the specialist IT distributor, has revealed."

Targeted ransomware doubled in 2022 - IT-Online

Source: https://it-online.co.za/2022/12/13/targeted-ransomware-doubled-in-2022/

From the Article: "Such a striking growth indicates that ransomware gangs have continued mastering their techniques – the infamous ones as well as those just entering the scene."

What is Threat Intelligence?

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Source: https://www.recordedfuture.com/threat-intelligence

From the Article: "Digital technologies lie at the heart of nearly every industry today. The automation and greater connectedness they afford have revolutionized the worlds economic and cultural institutions but theyve also brought risk in the form of cyberattacks."

A Security Vulnerability in the KmsdBot Botnet

Source: https://www.schneier.com/blog/archives/2022/12/a-security-vulnerability-in-the-kmsdbot-botnet.html

From the Article: "With no error-checking built in, sending KmsdBot a malformed command-—like its controllers did one day while Akamai was watching-—created a panic crash with an “index out of range” error."

Reassessing cyberwarfare. Lessons learned in 2022

Source: https://securelist.com/reassessing-cyberwarfare-lessons-learned-in-2022/108328/

From the Article: "At this point, it has become cliché to say that nothing in 2022 turned out the way we expected. We left the COVID-19 crisis behind hoping for a long-awaited return to normality and were immediately plunged into the chaos and uncertainty of a twentieth-century-style military conflict that posed serious risks of spreading over the continent. "

Secureworks® Cyber Defense Stories – The Weak Password Threat

Source: https://www.secureworks.com/resources/vd-irs-cyber-defense-stories-the-weak-password-threat

From the Article: "Watch this video to see how the Secureworks Adversary Group helped a state agency understand where they had gaps in their cyber defenses."

Threat Intelligence Executive Report 2022 Vol. 6

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Source: https://www.secureworks.com/resources/rp-irs-threat-intelligence-report-2022-vol-6

From the Article: "The Secureworks® Counter Threat Unit™ (CTU) researchers frequently serve as expert resources for the media, publish technical analyses for the security community, and speak about emerging threats at security conferences."

Crooks use HTML smuggling to spread QBot malware via SVG files

Source: https://securityaffairs.co/wordpress/139658/cyber-crime/qbot-html-smuggling-svg.html

From the Article: "Talos researchers uncovered a phishing campaign distributing the QBot malware using a new technique that leverages Scalable Vector Graphics (SVG) images embedded in HTML email attachments."

Chinese MirrorFace APT group targets Japanese political entities

Source: https://securityaffairs.co/wordpress/139698/apt/mirrorface-apt-group-targets-japan.html

From the Article: "ESET researchers recently discovered a spear-phishing campaign targeting Japanese political entities and attributed it to the Chinese-speaking APT group tracked as MirrorFace."

Citrix and NSA urge admins to fix actively exploited zero-day in Citrix ADC and Gateway

Source: https://securityaffairs.co/wordpress/139609/apt/citrix-adc-gateway-cve-2022-27518.html

From the Article: "Citrix urges customers to update their installs to fix actively exploited zero-day (CVE-2022-27518) in Citrix ADC and Gateway."

Twitter says recently leaked user data are from 2021 breach

Source: https://securityaffairs.co/wordpress/139574/data-breach/twitter-leaked-data-dated-2021-breach.html

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

From the Article: "Twitter confirmed that the recent leak of members' profile information resulted from the 2021 data breach disclosed in August 2022."

Chinese Cyberspies Targeted Japanese Political Entities Ahead of Elections
Source: https://www.securityweek.com/chinese-cyberspies-targeted-japanese-political-entities-ahead-elections

From the Article: "A Chinese cyberespionage group known as MirrorFace has been observed targeting Japanese political entities ahead of the House of Councillors election in July 2022."

Email Hack Hits 15,000 Business Customers of Australian Telecoms Firm TPG

Source: https://www.securityweek.com/email-hack-hits-15000-business-customers-australian-telecoms-firm-tpg

From the Article: "Australia's TPG Telecom this week announced that a threat actor has gained unauthorized access to a service hosting the email accounts of 15,000 customers."

VMware Patches VM Escape Flaw Exploited at Geekpwn Event

Source: https://www.securityweek.com/vmware-patches-vm-escape-flaw-exploited-geekpwn-event

From the Article: "Virtualization technology giant VMware on Tuesday shipped urgent updates to fix a trio of security problems in multiple software products, including a virtual machine escape bug exploited at the GeekPwn 2022 hacking challenge."

Hackers Bombard Open Source Repositories with Over 144,000 Malicious Packages

Source: https://thehackernews.com/2022/12/hackers-bombard-open-source.html

From the Article: "NuGet, PyPi, and npm ecosystems are the target of a new campaign that has resulted in over 144,000 packages being published by unknown threat actors."

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Android Malware Campaign Leverages Money-Lending Apps to Blackmail Victims

Source: https://thehackernews.com/2022/12/android-malware-campaign-leverages.html

From the Article: "A previously undocumented Android malware campaign has been observed leveraging money-lending apps to blackmail victims into paying up with personal information stolen from their devices."

Top 5 Web App Vulnerabilities and How to Find Them

Source: https://thehackernews.com/2022/12/top-5-web-app-vulnerabilities-and-how.html

From the Article: "Web applications, often in the form of Software as a Service (SaaS), are now the cornerstone for businesses all over the world. SaaS solutions have revolutionized the way they operate and deliver services, and are essential tools in nearly every industry, from finance and banking to healthcare and education."

Fortinet Warns of Active Exploitation of New SSL-VPN Pre-auth RCE Vulnerability

Source: https://thehackernews.com/2022/12/fortinet-warns-of-active-exploitation.html

From the Article: "Fortinet on Monday issued emergency patches for a severe security flaw affecting its FortiOS SSL-VPN product that it said is being actively exploited in the wild."

Researchers Uncover MirrorFace Cyber Attacks Targeting Japanese Political Entities

Source: https://thehackernews.com/2022/12/researchers-uncover-mirrorface-cyber.html

From the Article: "A Chinese-speaking advanced persistent threat (APT) actor codenamed MirrorFace has been attributed to a spear-phishing campaign targeting Japanese political establishments."

CISA researchers: Russia's Fancy Bear infiltrated US satellite network

Source: https://www.cyberscoop.com/apt28-fancy-bear-satellite/

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

From the Article: "Researchers at the Cybersecurity and Infrastructure Security Agency recently discovered suspected Russian hackers lurking inside a U.S. satellite network, raising fresh concerns about Moscow's intentions to infiltrate and disrupt the rapidly expanding space economy."

Pentagon Awards Strategic Contracts

Source: https://www.defense.gov/News/News-Stories/Article/Article/3237586/pentagon-awards-strategic-contracts/

From the Article: "To support production of kinetic capabilities needed to ensure national security, the Office of the Undersecretary of Defense for Acquisition and Sustainment is making targeted investments aimed at mitigating supply chain vulnerabilities, ranging from raw materials and chemical shortages to critical subcomponent suppliers."

CHIPS Act Spurs $200 Billion Investments in U.S. Semi Industry

Source: https://www.tomshardware.com/news/chips-act-spurs-200-billion-investments-in-us-semiconductor-industry

From the Article: "Semiconductor industry is reviving in the USA, says SIA."

NIST signs new research agreement for photonic chips

Source: https://www.fedscoop.com/nist-signs-new-semiconductor-rd-agreement-with-aim-photonics/

From the Article: "The National Institute of Standards and Technology (NIST) announced Tuesday a partnership with semiconductor manufacturer AIM Photonics that will give developers a critical new tool for designing faster chips that are key to laser-guided missiles, medical sensors and other advanced technologies."

Silent Data Corruption

Source: https://semiengineering.com/silent-data-corruption-2/

From the Article: "How to prevent defects that can cause errors."

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

GlobalFoundries Laying Off 148 Workers in Essex Junction

Source: https://www.sevendaysvt.com/vermont/globalfoundries-laying-off-148-workers-in-essex-junction/Content?oid=37189554

From the Article: "Semiconductor giant GlobalFoundries has informed Vermont that it is laying off 148 people in the state amid a corporate-wide downsizing. The cuts, detailed in a recent state filing, represent about 7 percent of the 2,000 people employed at the chipmaker's Essex Junction plant."

The Fevered Anti-China Attitude in Washington Is Going to Backfire - POLITICO

Source: https://www.politico.com/news/magazine/2022/12/15/china-tech-decoupling-sanctions-00071723

From the Article: "This technological decoupling, if done selectively, will help to preserve America's military edge, protect key U.S. industries from unfair competition, and push back on Beijing's human rights abuses."

America Won't Beat China by Becoming China | National Review

Source: https://www.nationalreview.com/2022/12/america-wont-beat-china-by-becoming-china/

From the Article: "America's world-leading digital technology compan ies and technologies were not the product of intentional design or bureaucratic initiatives."

Microsoft has found a whole load of IoT and industrial cyber flaws

Source: https://www.techradar.com/news/microsoft-has-found-a-whole-load-of-iot-and-industrial-cyber-flaws

From the Article: "Majority of industrial controllers are at risk from cyberattack, Microsoft warns"

Link back to Table of Contents

US Blacklists China Firms in AI Chip Sector, Russia Suppliers

Source: https://www.asiafinancial.com/us-blacklists-china-firms-in-ai-chip-sector-russia-suppliers

From the Article: "The US has added dozens of firms to its trade blacklist in a bid to curb China's military, human rights abuses, and block suppliers of the Russian military"

India Gaming to Become Global Semiconductor Powerhouse

Source: https://www.indrastra.com/2022/12/india-gaming-to-become-global.html

From the Article: "One of the main drivers of this effort has been the government's "Electronics System Design and Manufacturing" (ESDM) policy, which aims to increase domestic electronics production in India and reduce the country's reliance on imported semiconductors."

Ransomware Hackers Using New Way to Bypass MS Exchange ProxyNotShell Mitigations

Source: https://thehackernews.com/2022/12/ransomware-hackers-using-new-way-to.html

From the Article: "Threat actors affiliated with a ransomware strain known as Play are leveraging a never-before-seen exploit chain that bypasses blocking rules for ProxyNotShell flaws in Microsoft Exchange Server to achieve remote code execution (RCE) through Outlook Web Access (OWA)."

3D-IC Reliability Degrades With Increasing Temperature

Source: https://semiengineering.com/3d-ic-reliability-degrades-with-increasing-temperature/

From the Article: "Electromigration and other aging factors become more complicated along the z axis."

Sun Tzu, competition with China and the art of acquisition

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Source: https://breakingdefense.com/2022/12/sun-tzu-competition-with-china-and-the-art-of-acquisition/

From the Article: "This September, 20 leading experts on defense acquisition gathered for a workshop on how the US can best compete with China. Convened by the Acquisition Innovation Research Center at the Stevens Institute of Technology, the group took inspiration from the iconic Chinese work on strategy, Sun Tzu's Art of War."

Nearly 200 billion in investments already attributed to chips and science act

Source: https://electronics360.globalspec.com/article/19079/nearly-200-billion-in-investments-already-attributed-to-chips-and-science-act

From the Article: "The CHIPS and Science Act has already attracted more than 40 new semiconductor ecosystem projects across the U.S. to the tune of $186.6 billion, according to the Semiconductor Industry Association (SIA)."

How to spot AI-generated text

Source: https://www.technologyreview.com/2022/12/19/1065596/how-to-spot-ai-generated-text/

From the Article: "The internet is increasingly awash with text written by AI software. We need new tools to detect it."

Chip Industry's Technical Paper Roundup: Dec. 13

Source: https://semiengineering.com/chip-industrys-technical-paper-roundup-dec-13/

From the Article: "2D materials special issue; measuring direct bonding at wafer scale; information flow for HW; hafnium oxide-based FeFETs for in-memory; fully rubbery Schottky diodes and ICs; layered HW security for cloud and edge; neural architecture and HW accelerator co-design framework."

WHO, WIPO, WTO Call For Innovation And Cooperation To Support Timely Access To Pandemic Products

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Source: https://www.wipo.int/policy/en/news/global_health/2022/news_0004.html

From the Article: "The Joint Technical Symposium held on 16 December by the World Health Organization (WHO), World Intellectual Property Organization (WIPO) and the World Trade Organization (WTO) highlighted that the world can move quickly when driven by a crisis situation, such as the COVID-19 pandemic."

Russia's Trident Ursa (aka Gamaredon APT) Cyber Conflict Operations Unwavering Since Invasion of Ukraine

Source: https://unit42.paloaltonetworks.com/trident-ursa/

From the Article: "Since our last blog in early February covering the advanced persistent threat (APT) group Trident Ursa (aka Gamaredon, UAC-0010, Primitive Bear, Shuckworm), Ukraine and its cyber domain has faced ever-increasing threats from Russia. Trident Ursa is a group attributed by the Security Service of Ukraine to Russia's Federal Security Service."

The March Toward Chiplets

Source: https://semiengineering.com/the-march-toward-chiplets/

From the Article: "The benefits of heterogenous integration are well understood, but getting there isn't easy."

Senate passes $847B defense bill, forcing Biden's hand on vaccine mandate

Source: https://www.politico.com/news/2022/12/15/senate-passes-847b-defense-bill-forcing-bidens-hand-on-vaccine-mandate-00074246

From the Article: "The compromise National Defense Authorization Act now heads to the White House for Biden's signature."

Microsoft Details Gatekeeper Bypass Vulnerability in Apple macOS Systems

Source: https://thehackernews.com/2022/12/microsoft-details-gatekeeper-bypass.html

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

From the Article: "Microsoft has disclosed details of a now-patched security flaw in Apple macOS that could be exploited by an attacker to get around security protections imposed to prevent the execution of malicious applications."

ASML's Taiwan Expansion Signals Chip Sector's Next Big Leap

Source: https://www.asiafinancial.com/asmls-taiwan-expansion-signals-chip-sectors-next-big-leap

From the Article: "The Dutch chip-making machine manufacturer is planning ways to make even smaller, faster chips as it deepens its links with the industry's most important hub, Taiwan"

Top bug bounty platforms for organizations to improve security

Source: https://cybersecurity.att.com/blogs/security-essentials/top-bug-bounty-platforms-for-organizations-to-improve-security

From the Article: "As mentioned in Wikipedia: "A bug bounty program is a deal offered by many websites, organizations and software developers by which individuals can receive recognition and compensation for reporting bugs, especially those pertaining to security exploits and vulnerabilities"."

Supply Chain Weekly Wrap-Up 12/09/2022-12/15/2022

Source: https://www.allthingssupplychain.com/supply-chain-weekly-wrap-up-12-09-2022-12-15-2022/

From the Article: "Gilimex Inc a Vietnamese warehouse equipment manufacturer is suing Amazon for $280 million, claiming that the e-commerce giant backed away from agreements made early in 2020 to support the supplier with large amounts of capital for new purchases."

2023 Anomali Predictions: New Risks to Put Added Pressure on Enterprise Defenders

Source: https://www.anomali.com/blog/2023-anomali-predictions-new-risks-to-put-added-pressure-on-enterprise-defenders

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

From the Article: "Cybersecurity has a way of surprising us with the unexpected so I wouldn't be surprised to see a completely new kind of security threat emerge in 2023. But as the ongoing cat-and-mouse game between attackers and defenders unfolds, certain scenarios are already coming into view."

MoneyMonger: Predatory Loan Scam Campaigns Move to Flutter

Source: https://zimpstage.wpengine.com/blog/moneymonger-predatory-loan-scam-campaigns-move-to-flutter/

From the Article: "Flutter, the open-source user interface (UI) software kit for cross-platform mobile applications, has helped drive new mobile applications onto the market. This modern mobile application framework removes many barriers to creating multi-platform applications, and developers can create native mobile apps with only one codebase."

Medical data is moving to telemedicine, but security hasn't kept up

Source: https://digitalisationworld.com/blogs/57169/medical-data-is-moving-to-telemedicine-but-security-hasnt-kept-up#new_tab

From the Article: "The post Medical data is moving to telemedicine, but security hasn't kept up appeared first on Zimperium."

Mobile Threat Patterns Across Australia | 2022 Q3 Analysis

Source: https://www.brighttalk.com/webcast/19320/565880

From the Article: "No matter the device OS or ownership, the mobile attack surface is increasingly under attack. From spear phishing attacks successfully targeting critical services to feature-rich mobile malware infecting mobile devices to advanced spyware, the threat vector against federal & state systems in Australia continues to get larger with each mobile endpoint connected."

Vulnerability Spotlight: Authentication bypass and enumeration vulnerabilities in Ghost CMS

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Source: https://blog.talosintelligence.com/vulnerability-spotlight-authentication-bypass-and-enumeration-vulnerabilities-in-ghost-cms/

From the Article: "Cisco Talos recently discovered two vulnerabilities in Ghost CMS, one authentication bypass vulnerability and one enumeration vulnerability."

Threat Spotlight: XLLing in Excel - threat actors using malicious add-ins

Source: https://blog.talosintelligence.com/xlling-in-excel-malicious-add-ins/

From the Article: "For decades, Microsoft Office applications have served as one of the most significant entry points for malicious code. Malicious actors have continued to utilize Visual Basic for Applications (VBA) macros, despite automatic warnings to users after opening Office documents containing code."

Threat Round up for December 9 to December 16

Source: https://blog.talosintelligence.com/threat-roundup-1209-1216/

From the Article: "Today, Talos is publishing a glimpse into the most prevalent threats we've observed between Dec. 9 and Dec. 16. As with previous roundups, this post isn't meant to be an in-depth analysis."

BrandPost: The Next Big Attack Vector: Your Supply Chain

Source: https://www.csoonline.com/article/3684009/the-next-big-attack-vector-your-supply-chain.html

From the Article: "There’s an old security adage: a chain is only as strong as its weakest link. The sentiment long predates Information and Communications Technology (ICT), but it’s never been more relevant. With modern ICT connecting millions of systems worldwide, there are exponentially more “links” to worry about."

Social media use can put companies at risk: Here are some ways to mitigate the danger

Source: https://www.csoonline.com/article/3683868/how-social-media-puts-companies-at-risk-and-how-to-mitigate-it.html

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

From the Article: "We live in a social world, but should our businesses? For many, the answer to that is increasingly no—that's why laws and regulations have recently been put in place restricting access to some social media in certain situations because of the hidden risks of these seemingly innocuous platforms."

BrandPost: Why a Culture of Awareness and Accountability Is Essential to Cybersecurity

Source: https://www.csoonline.com/article/3683789/why-a-culture-of-awareness-and-accountability-is-essential-to-cybersecurity.html

From the Article: "Effective cybersecurity relies only in part on technology. Even as tools and systems become more powerful, avoiding security mishaps is still largely dependent on people doing the right thing."

BrandPost: Keeping your retail business safe from the cyber grinches

Source: https://www.csoonline.com/article/3683589/keeping-your-retail-business-safe-from-the-cyber-grinches.html

From the Article: "It’s not just retailers looking forward to the holiday shopping season; it’s also a time of plenty for cunning cybercriminals. While security and IT teams are working harder to manage online traffic spikes, maintain corporate operations and much more during this busy period, bad actors are taking the opportunity to launch targeted attacks."

Report highlights serious cybersecurity issues with US defense contractors

Source: https://www.csoonline.com/article/3682673/clear-and-present-danger-report-highlights-serious-cybersecurity-issues-with-us-defense-contractors.html

From the Article: "When a company engages in business with a government, especially with the defense sector of that government, one should expect that security surrounding the engagement would be a serious endeavor."

Weekly Cyber Threat Report, December 12 – 17, 2022

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Source: https://cyberintelmag.com/threat-intelligence/weekly-cyber-threat-report-december-12-17-2022/

From the Article: "This week's good news includes Apple releasing security updates to address a new 0-day flaw, Google coming up with an OVS-Scanner tool to find open source flaws, Adobe fixing 38 vulnerabilities in enterprise software products, Lego addressing dangerous API flaws in BrickLink service, and much more."

Japanese Politicians Being Targeted by Hackers With Novel MirrorStealer Malware

Source: https://cyberintelmag.com/malware-viruses/japanese-politicians-being-targeted-by-hackers-with-novel-mirrorstealer-malware/

From the Article: "Before the House of Councilors election in July 2022, a hacker gang known as MirrorFace had been targeting Japanese lawmakers using a previously unknown credentials stealer known as "MirrorStealer.""

Chris Inglis to resign as national cyber director

Source: https://www.cyberscoop.com/inglis-resign-national-cyber-director/

From the Article: "National Cyber Director Chris Inglis plans to step down from his position as a senior White House cybersecurity adviser, a decision first reported by CNN and confirmed to CyberScoop by three sources with direct knowledge of the matter."

Cybercriminals are Targeting Gamers Next

Source: https://www.cysecurity.news/2022/12/cybercriminals-are-targeting-gamers-next.html

From the Article: "It has been reported that while the objectives of those looking to break into consumers' personal information and steal their financial information will remain the same next year, they will be targeting new people and redeveloping platforms to try to get around the defenses set in place. "

Hacking Group Takes Down "Antwerp" from Website

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Source: https://www.cysecurity.news/2022/12/hacking-group-takes-down-antwerp-from.html

From the Article: "The City of Antwerp is no longer listed as one of the organizations that the hacker group Play has compromised on its website. Uncertainty surrounds the meaning of this."

A Huge DDoS Network was Taken Down by the US DOJ

Source: https://www.cysecurity.news/2022/12/a-huge-ddos-network-was-taken-down-by.html

From the Article: "According to the US Department of Justice (DOJ), 48 domains were seized after it was discovered that they were offering distributed denial of service (DDoS) attacks on-demand as a service that criminals could exploit."

New Botnet Targeting Minecraft Servers Could be a Threat to Enterprises

Source: https://www.cysecurity.news/2022/12/new-botnet-targeting-minecraft-servers.html

From the Article: "Enterprises are being affected significantly more by the constant spread of a newly discovered botnet, that is apparently targeting private Minecraft Java servers than simply bumming out a biome. "

Trojanized Windows 10 Installer Utilized in Cyberattacks Against Ukrainian Government Entities

Source: https://www.cysecurity.news/2022/12/trojanized-windows-10-installer.html

From the Article: "Ukraine's government has been compromised as part of a new campaign that used trojanized versions of Windows 10 installer files to conduct post-exploitation activities. "

Social Blade Confirms Data Breach

Source: https://www.cysecurity.news/2022/12/social-blade-confirms-data-breach.html

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

From the Article: "The company Social Blade has disclosed a security breach after a group of threat actors offered to sell a database illegally obtained from the company's systems. "

NSA, CISA Concerns Over Security Risks Against 5G Network Slicing

Source: https://www.cysecurity.news/2022/12/nsa-cisa-concerns-over-security-risks.html

From the Article: "The National Security Agency (NSA) and the Cybersecurity and Infrastructure Security Agency (CISA) have recently released new guidelines regarding cybersecurity threats pertaining to 5G network slicing. "

How Can Schools Minimize Cybersecurity Risks?

Source: https://www.cysecurity.news/2022/12/how-can-schools-minimize-cybersecurity.html

From the Article: "Cyberattacks are now a daily threat to K-12 schools, and the problem may worsen as educators rely more on technology for teaching and learning, and as hackers become more sophisticated. "

Hackers Leaked Stolen Data of 5.7M Gemini Users

Source: https://www.cysecurity.news/2022/12/hackers-leaked-stolen-data-of-57m.html

From the Article: "Gemini crypto exchange recently made an announcement this week that its customers have been victimized in a phishing campaign after a group of malicious actors collected their personal credentials by breaching a third-party vendor. "

This Linux-Targeting Malware is Becoming Even More Potent

Source: https://www.cysecurity.news/2022/12/this-linux-targeting-malware-is.html

From the Article: "A trojan software has been added to the capabilities of a cryptomining malware campaign that targets Linux-based devices and cloud computing instances,

potentially making attacks more severe."

Supply Chain Risks Got You Down? Keep Calm and Get Strategic!

Source: https://www.darkreading.com/risk/supply-chain-risks-got-you-down-keep-calm-and-get-strategic-

From the Article: "Security leaders must maintain an effective cybersecurity strategy to help filter some of the noise on new vulnerabilities."

Ransomware Attackers Bypass Microsoft's ProxyNotShell Mitigations With Fresh Exploit

Source: https://www.darkreading.com/application-security/ransomware-attackers-bypass-microsoft-mitigation-proxynotshell-exploit

From the Article: "The Play ransomware group was spotted exploiting another little-known SSRF bug to trigger RCE on affected Exchange servers."

Heartland Alliance Provides Notice of Data Security Incident

Source: https://www.darkreading.com/attacks-breaches/heartland-alliance-provides-notice-of-data-security-incident

From the Article: "Heartland Alliance ("Heartland"), a social justice and human rights organization headquartered in Chicago, Illinois, has experienced a data security incident that may have involved personal and protected health information belonging to employees, directors, independent contractors, and certain individuals who sought health care or participated in other Heartland programs."

Paying Ransom: Why Manufacturers Shell Out to Cybercriminals

Source: https://www.darkreading.com/zscaler/paying-ransom-why-manufacturers-shell-out-to-cybercriminals

From the Article: "Lower cybersecurity awareness coupled with vulnerable OT gear makes manufacturers tempting targets, but zero trust can blunt attackers' advantages."

Link back to Table of Contents

NATO-Member Oil Refinery Targeted in Russian APT Blitz Against Ukraine

Source: https://www.darkreading.com/attacks-breaches/nato-oil-refinery-russian-apt-blitz-against-ukraine

From the Article: "Security Service-backed Trident Ursa APT group shakes up tactics in its relentless cyberattacks against Ukraine."

Searchlight Security Changes Name to Searchlight Cyber and Launches New Brand

Source: https://www.darkreading.com/threat-intelligence/searchlight-security-changes-name-to-searchlight-cyber-and-launches-new-brand

From the Article: "Searchlight Cyber announces rebrand that reflects its status as a fast-growing cybersecurity business."

How AI/ML Can Thwart DDoS Attacks

Source: https://www.darkreading.com/dr-tech/how-ai-ml-can-thwart-ddos-attacks

From the Article: "When properly designed and trained, artificial intelligence and machine learning can help improve the accuracy of distributed denial-of-service detection and mitigation."

'Blindside' Attack Subverts EDR Platforms From Windows Kernel

Source: https://www.darkreading.com/attacks-breaches/-blindside-attack-subverts-edr-platforms-windows-kernel

From the Article: "The technique loads a nonmonitored and unhooked DLL, and leverages debug techniques that could allow for running arbitrary code."

AWS Elastic IP Transfer Feature Gives Cyberattackers Free Range

Source: https://www.darkreading.com/cloud/aws-elastic-ip-transfer-feature-cyberattackers-free-range

Link back to Table of Contents

The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

From the Article: "Threat actors can take over victims' cloud accounts to steal data, or use them for command-and-control for phishing attacks, denial of service, or other cyberattacks."

Sophisticated DarkTortilla Malware Serves Imposter Cisco, Grammarly Pages

Source: https://www.darkreading.com/attacks-breaches/darktortilla-malware-imposter-cisco-grammarly-phishing

From the Article: "Sites spoofing Grammarly and a Cisco webpage are spreading the DarkTortilla threat, which is filled with follow-on malware attacks."

Threat Intelligence Through Web Scraping

Source: https://www.darkreading.com/threat-intelligence/threat-intelligence-through-web-scraping

From the Article: "Bright Data CEO Or Lenchner discusses how security teams are utilizing public Web data networks to safeguard their organizations from digital risks."

Malicious Python Trojan Impersonates SentinelOne Security Client

Source: https://www.darkreading.com/vulnerabilities-threats/malicious-python-trojan-impersonates-sentinelone-security-client

From the Article: "A fully functional SentinelOne client is actually a Trojan horse that hides malicious code within; it was found lurking in the Python Package Index repository ecosystem."

Holiday Spam, Phishing Campaigns Challenge Retailers

Source: https://www.darkreading.com/attacks-breaches/holiday-spam-phishing-campaigns-challenge-retailers

From the Article: "Revived levels of holiday spending have caught the eye of threat actors who exploit consumer behaviors and prey on the surge of online payments and

digital activities during the holidays."

Cyber Threats Loom as 5B People Prepare to Watch World Cup Final

Source: https://www.darkreading.com/attacks-breaches/cyberthreats-loom-5b-people-watch-world-cup-final

From the Article: "The 2022 FIFA Men's World Cup final in Qatar will be the most-watched sporting event in history — but will cybercriminals score a hat trick off its state-of-the-art digital footprint?"

New Botnet Targeting Minecraft Servers Poses Potential Enterprise Threat

Source: https://www.darkreading.com/attacks-breaches/new-botnet-targeting-minecraft-serversa-potential-enterprise-threat-

From the Article: "The 2022 FIFA Men's World Cup final in Qatar will be the most-watched sporting event in history — but will cybercriminals score a hat trick off its state-of-the-art digital footprint?"

Clare O'Neil on national security amid cyber hacks and threats to democracy

Source: https://www.theguardian.com/australia-news/audio/2022/dec/17/clare-oneil-on-national-security-amid-cyber-hacks-and-threats-to-democracy

From the Article: "In the final episode of Australian Politics for 2022, political editor Katharine Murphy speaks to the minister for home affairs and cyber security Clare O'Neil about the strategic challenges for Australia and the region. "

4images 1.9 Remote Command Execution

Source: https://packetstormsecurity.com/files/170323/4images19-exec.txt

From the Article: "4images version 1.9 suffers from a remote command execution vulnerability."

Link back to Table of Contents

New Supply Chain Attack Uses Python Package Index "aioconsol"

Source: https://www.fortinet.com/blog/threat-research/new-supply-chain-attack-uses-python-package-index-aioconsol

From the Article: "FortiGuardLabs recently discovered a 0-day attack in a PyPI package called "aioconsol.""

Cybersecurity Guidance for Financial Services Industry Leaders in 2023

Source: https://www.fortinet.com/blog/ciso-collective/cybersecurity-guidance-for-financial-services-industry-leaders-in-2023

From the Article: "Now that DORA has been adopted, financial firms will be required to ensure that they can withstand, respond to, and recover from all types of threats and disruptions. "

Your Holiday Guide to Safe Cybershopping

Source: https://www.fortinet.com/blog/industry-trends/holiday-guide-safe-cyber-shopping

From the Article: "Learn tips and best practices to secure your online shopping experience this holiday season."

Proactively Detect and Respond to External Threats Using FortiRecon Digital Risk Protection Service

Source: https://www.fortinet.com/blog/business-and-technology/detect-and-respond-to-external-threats-using-fortirecon-digital-risk-protection

From the Article: "Your external attack surfaces provide numerous potential intrusion points that cybercriminals regularly exploit to penetrate an organization."

MSG Allegedly Used Facial Recognition to Remove Rival Attorney From Rockettes Show

Source: https://gizmodo.com/mgs-facial-recognition-msg-rockettes-show-1849919528

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

From the Article: "An attorney working for a law firm taking legal action against MSG Entertainment claims she was spotted by the company's facial recognition security system while attending a Rockettes show with her daughter and was ultimately denied entry."

A look back at 2022's top tech and cyber stories

Source: https://govmatters.tv/a-look-back-at-2022s-top-tech-and-cyber-stories/

From the Article: "Jill Aitoro, senior vice president of content strategy for CyberRisk Alliance, and Ross Wilkers, senior staff reporter for Washington Technology, discuss the biggest federal tech and cyber news of 2022 and the issues to watch for 2023."

Data breach at Social Blade confirmed. Hacker offers to sell database on underground website

Source: https://www.bitdefender.com/blog/hotforsecurity/data-breach-at-social-blade-confirmed-hacker-offers-to-sell-database-on-underground-website/

From the Article: "Social media analytics service Social Blade has confirmed that it is investigating a security breach, after a hacker offered its user database for sale on an underground criminal website."

Backup saves the day after crime author loses laptop in blizzard

Source: https://grahamcluley.com/backup-saves-the-day-after-crime-author-loses-laptop-in-blizzard/

From the Article: "Celebrated crime author Ann Cleeves turned to Twitter this week, desperate for help."

GitHub Attack Allowed Attackers to Steal Okta's Source Code

Source: https://www.hackread.com/okta-source-code-github-attack/

From the Article: "Okta has, however, confirmed that attackers couldn't access its

customer data or services."

"GodFather" Hits Banks, Crypto Wallets Apps as Android Trojan Emerges

Source: https://www.hackread.com/godfather-android-trojan-banks-crypto-apps/

From the Article: "Researchers believe that GodFather could be a successor of another banking trojan called Anubis, which had its source code leaked in January 2019 on an underground hacking forum."

Russian Killnet Hackers Claim Data Theft of FBI Agents

Source: https://www.hackread.com/russian-killnet-hackers-fbi-agents/

From the Article: "On Telegram, Killnet hackers have leaked a text file showing the login credentials of 10,000 individuals whom they claim are FBI agents."

Hacked Ring Cameras Used in Livestreaming Swatting Attacks

Source: https://www.hackread.com/hacked-ring-cameras-swatting-attacks/

From the Article: "Per the police, the two suspects were aided by a third man who obtained the login credentials of victims' Yahoo accounts and identified if they owned a Ring doorbell camera."

Instagram Rolls Out dedicated Page To Help Users Regain Hacked Accounts

Source: https://www.hackread.com/instagram-hacked-accounts-regain/

From the Article: "Instagram has launched new account support for users who may have lost access to their accounts. "

Microsoft Alert: DDoS Botnet Hit Private Minecraft Servers

Source: https://www.hackread.com/microsoft-ddos-botnet-minecraft-servers/

Link back to Table of Contents

From the Article: "Dubbed "MCCrash" by Microsoft, the DDoS botnet is currently targeting private Minecraft servers globally."

Hackers Breach TPG Telecoms' Email Host to Steal Client Data

Source: https://www.hackread.com/hackers-tpg-telecoms-email-host-breach/

From the Article: "The TGP telecom giant based in North Ryde, Australia revealed that up to 15,000 iiNet and Westnet business customers have been impacted by the breach."

Gemini - 5,274,214 breached accounts

Source: https://haveibeenpwned.com/PwnedWebsites#Gemini

From the Article: "In late 2022, data allegedly taken from the Gemini crypto exchange was posted to a public hacking forum. The data consisted of email addresses and partial phone numbers, which Gemini later attributed to an incident at a third-party vendor (the vendor was not named)."

Recently Discovered RisePro Malware Is a Vidar Stealer Derivative

Source: https://heimdalsecurity.com/blog/recently-discovered-risepro-malware-is-a-vidar-stealer-derivative/

From the Article: "RisePro, a new information-stealing malware, was recently observed on a dark web forum run by Russian cybercriminals. Since December 13, the virus has been offered for sale as a log credential stealer on underground forums, leading many to believe it is a clone of the Vidar Stealer."

Agenda Ransomware Steals Sensitive Data from Critical Infrastructure

Source: https://heimdalsecurity.com/blog/agenda-ransomware-steals-sensitive-data-from-critical-infrastructure/

From the Article: "This year, many ransomware-as-a-service groups, including Agenda and Qilin, have developed versions of their ransomware in Rust. Like its Golang

counterpart, the Rust variant of Agenda has targeted essential industries."

Raspberry Robin Worm Uses Fake Malware to Evade Detection

Source: https://heimdalsecurity.com/blog/raspberry-robin-fake-malware-avoid-detection/

From the Article: "Threat actors started using fake malware to confuse researchers and avoid being analyzed by detection systems. The new technique involves dropping a fake payload when the malware senses it`s being run into a sandbox and analyzed. If the analysis doesn`t seem to take place, real Raspberry Robin malware is launched."

Additional sources:
https://www.bleepingcomputer.com/news/security/raspberry-robin-worm-drops-fake-malware-to-confuse-researchers/

New Microsoft Exchange Exploit Used by Ransomware Gang to Breach Servers

Source: https://heimdalsecurity.com/blog/new-microsoft-exchange-exploit-used-by-ransomware-gang-to-breach-servers/

From the Article: "A group of threat actors known as Play ransomware is using a new exploit in Microsoft Exchange to breach servers. The exploit chain bypasses ProxyNotShell URL rewrite mitigations to gain remote code execution (RCE) on vulnerable servers."

Threat Actors Target Ukraine's DELTA Military System with Info-Stealing Malware

Source: https://heimdalsecurity.com/blog/threat-actors-target-ukraines-delta-military-system-with-info-stealing-malware/

From the Article: "Hackers used an email account belonging to the Ukrainian Ministry of Defense for launching a phishing campaign against DELTA. On December 18th, CERT-UA (Computer Emergency Response Team of Ukraine) warned that the DELTA military system was targeted with info-stealing malware."

Australian Fire and Rescue Service Confirms Cyber Attack

Link back to Table of Contents

Source: https://heimdalsecurity.com/blog/australian-fire-and-rescue-service-confirms-cyber-attack/

From the Article: "Last week, while dealing with a widespread IT outage, the fire and rescue service in the state of Victoria (FRV), Australia, has confirmed being the victim of a cyber attack."

SevenRooms Restaurant Platform Sufferes a Data Breach

Source: https://heimdalsecurity.com/blog/sevenrooms-restaurant-platform-sufferes-a-data-breach/

From the Article: "SevenRooms restaurant platform confirmed that it was affected by a data breach after hackers posted stolen data for sale on the darknet."

SECURITY ALERT: Aikido Wiperware Leverages Security Controls Vulnerability to Delete System Files with User-Type Privileges

Source: https://heimdalsecurity.com/blog/aikido-wiperware/

From the Article: "In the wake of SafeBreach's Aikido Wiperware vulnerability announcement back in early December, many have begun to suspect the possibility of pseudo-ransomware making a comeback. "

BlackCat Ransomware Targets Colombian Energy Supplier EPM

Source: https://heimdalsecurity.com/blog/blackcat-ransomware-targets-colombian-energy-supplier-epm/

From the Article: "Empresas Públicas de Medellín (EPM), a Colombian energy provider, suffered from a BlackCat/ALPHV ransomware assault on Monday, which negatively impacted business operations and shut down internet services."

Microsoft: Minecraft Servers Are Being Attacked by a Cross-Platform DDoS Botnet

Source: https://heimdalsecurity.com/blog/microsoft-minecraft-servers-are-being-attacked-by-a-cross-platform-ddos-botnet/

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

From the Article: "On Thursday, Microsoft warned users about a cross-platform botnet that targets private Minecraft servers with distributed denial-of-service (DDoS) attacks. The botnet, known as MCCrash, has a special technique for propagating that allows it to infect Linux-based computers despite its origins in malicious software downloaded on Windows hosts."

Ukrainian Government Hacked Through Malicious Windows ISO Files

Source: https://heimdalsecurity.com/blog/ukrainian-government-hacked-malicious-iso-files/

From the Article: "Ukrainian government networks were infected via trojanized ISO files posing as legitimate Windows 10 installers and several governmental institutions were hacked."

Phishing Attack Uses Facebook Posts to Evade Email Security

Source: https://heimdalsecurity.com/blog/phishing-attack-uses-facebook-posts-to-evade-email-security/

From the Article: "Phishing scams have become more complex over time, and scammers are finding new ways to obtain information about their victims. This new phishing campaign is no different."

The Data of 5.7 Million Gemini Users Leaked by Threat Actors

Source: https://heimdalsecurity.com/blog/the-data-of-5-7-million-gemini-users-leaked-by-threat-actors/

From the Article: "This week, the Gemini cryptocurrency exchange disclosed that after a threat actor obtained the clients' data from a third-party vendor, they became the victim of phishing attacks. "

8 Social Media Influencers Accused of Securities Fraud in the US

Source: https://heimdalsecurity.com/blog/8-social-media-influencers-accused-of-

securities-fraud-in-the-us/

From the Article: "Authorities from the Southern District of Texas accused eight men of committing securities fraud by participating in a “pump and dump” scheme."

Simeio collaborates with SailPoint to address today’s security, risk, and compliance needs

Source: https://www.helpnetsecurity.com/2022/12/22/simeio-sailpoint/

From the Article: "Simeio partners with SailPoint to strengthen enterprise identity governance adoption and implementation of simplified, interoperable, and automated identity security programs."

Omer Grossman joins CyberArk as CIO

Source: https://www.helpnetsecurity.com/2022/12/22/cyberark-omer-grossman/

From the Article: "CyberArk appoints Omer Grossman as Global Chief Information Officer (CIO), bringing strong cloud infrastructure and cybersecurity resiliency experience to this role. After serving in the Israel Defense Forces (IDF) for more than 25 years, Grossman will lead CyberArk’s Global Information Technology group."

The benefit of adopting a hacker mindset for building security strategies

Source: https://www.helpnetsecurity.com/2022/12/21/hacker-mindset-building-security-strategies-video/

From the Article: "As VP of Research at Pentera, Alex Spivakovsky leads a team of former pen-testers, red-teamers, and incident response experts whose job is to bypass existing security controls. "

Make sure your company is prepared for the holiday hacking season

Source: https://www.helpnetsecurity.com/2022/12/20/company-prepared-holiday-hacking-season/

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

From the Article: "We're coming to that time of the year when employees are excited about the holidays and taking time off to be with their loved ones. But while employees are preparing for some rest and relaxation, hackers are gearing up for their busy season."

Connected homes are expanding, so is attack volume

Source: https://www.helpnetsecurity.com/2022/12/20/connected-homes-attack-volume/

From the Article: "78% Americans report unsafe online behaviors that open them up to cyber threats, such as reusing or sharing passwords, skipping software updates and more – a 14% increase from just two years ago, according to Comcast."

85% of attacks now use encrypted channels

Source: https://www.helpnetsecurity.com/2022/12/19/attacks-encrypted-channels/

From the Article: "Malware continues to pose the greatest threat to individuals and businesses across nine key industries, with manufacturing, education and healthcare being the most commonly targeted, according to Zscaler."

5 cybersecurity trends accelerating in 2023

Source: https://www.helpnetsecurity.com/2022/12/19/5-cybersecurity-trends-accelerating-in-2023/

From the Article: "Netwrix has released key cybersecurity trends that will affect organizations of all sizes in 2023. Here are five specific trends that you need to be aware of: The business of cybercrime will be further professionalized."

Anomali unveils new solutions and capabilities to strengthen cyber resiliency for users

Source: https://www.helpnetsecurity.com/2022/12/19/anomali-solutions-and-capabilities/

From the Article: "Anomali unveiled new capabilities to extend an organization's visibility across their entire internal and external digital footprint with an integrated risk assessment that protects against potential attacks."

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Action1 platform upgrades enable organizations to mitigate security and non-compliance risks

Source: https://www.helpnetsecurity.com/2022/12/19/action1-new-version/

From the Article: "Action1 released the new version of its solution, helping internal IT departments and managed service providers (MSPs) intelligently automate patching and remediation of security vulnerabilities across their endpoints and monitor patching results in real-time."

Week in review: Citrix and Fortinet RCEs, Microsoft fixes exploited zero-day

Source: https://www.helpnetsecurity.com/2022/12/18/week-in-review-citrix-and-fortinet-rces-microsoft-fixes-exploited-zero-day/

From the Article: "Here's an overview of some of last week's most interesting news, articles, interviews and videos: Vulnerability with public PoC affects Cisco IP phones, fix unavailable (CVE-2022-20968) A high-risk stack overflow vulnerability (CVE-2022-20968) may allow attackers to DoS or possibly even execute code remotely on Cisco 7800 and 8800 Series IP phones, the company has confirmed."

Lack of key domain security measures leaves organizations at risk

Source: https://www.helpnetsecurity.com/2022/12/16/domain-security-measures-video/

From the Article: "In this Help Net Security video, Ihab Shraim, CTO at CSC, talks about how 75% of the Forbes Global 2000 are exposing themselves to significant enterprise risks as third parties maliciously register their brands, and they fail to implement key domain security measures."

Executives take more cybersecurity risks than office workers

Source: https://www.helpnetsecurity.com/2022/12/16/executives-take-more-cybersecurity-risks-than-office-workers/

From the Article: "Ivanti worked with cybersecurity experts and surveyed 6,500

executive leaders, cybersecurity professionals, and office workers to understand the perception of today's cybersecurity threats and find out how companies are preparing for yet-unknown future threats."

F5 Distributed Cloud App Infrastructure Protection detects vulnerabilities in real time

Source: https://www.helpnetsecurity.com/2022/12/16/f5-distributed-cloud-app-infrastructure-protection/

From the Article: "F5 launches F5 Distributed Cloud App Infrastructure Protection (AIP), a cloud workload protection solution that expands application observability and protection to cloud-native infrastructures. "

Malwarebytes strengthens threat prevention capabilities in Nebula platform

Source: https://www.helpnetsecurity.com/2022/12/16/malwarebytes-nebula/

From the Article: "Malwarebytes expands Malwarebytes Nebula platform with additional threat prevention capabilities developed specifically for resource constrained organizations to reduce attack surfaces from a simple, easy-to-use cloud-based interface."

5 tips for building a culture of cybersecurity accountability

Source: https://www.helpnetsecurity.com/2022/12/15/5-tips-for-building-a-culture-of-cybersecurity-accountability-video/

From the Article: "In this Help Net Security video, Corey Nachreiner, CSO at WatchGuard, talks about how effective cybersecurity often boils down to doing the basics: patching, updating, and following day-to-day best practices for using applications and systems."

Distractions at work can have serious cybersecurity implications

Source: https://www.helpnetsecurity.com/2022/12/15/distracted-employees-cybersecurity/

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

From the Article: "Distracted employees are twice as likely to do the bare minimum for security at work, according to 1Password. The findings reveal that sustained burnout, now paired with high levels of distraction, has critical implications for workplace security."

Congress' $1.7T omnibus makes accelerating emerging defense tech a national priority

Source: https://defensescoop.com/2022/12/21/congress-1-7t-omnibus-makes-accelerating-emerging-defense-tech-a-national-priority/

From the Article: "Released by congressional appropriators Tuesday, the roughly $1.7 trillion 2023 omnibus spending bill would provide the Defense Department with more than $797 billion in total base discretionary funding, much of which is aimed at boosting its tech portfolio. The legislation is expected to pass and be signed into law by President Biden in the coming days."

Pentagon's CMMC program launch faces delay as OMB rulemaking review shifts to January

Source: https://insidecybersecurity.com/share/14197

From the Article: "The Defense Department is in the process of making changes to its Cybersecurity Maturity Model Certification program following an internal review in 2021."

A strategy compass for companies - Supply Chain Movement

Source: https://www.supplychainmovement.com/strategy-compass-companies/

From the Article: "Research by McKinsey in 2011 revealed that just 35 percent of companies have a successful strategy which enables them to beat the competition. And only 20 percent of companies explicitly interconnect their strategy, product portfolio and the resources required, i.e. supply chain management."

The 3 big initiatives topping the 2023 supply chain to do list

Source: https://epsnews.com/2022/12/21/the-3-big-initiatives-topping-the-2023-supply-chain-to-do-list/

Link back to Table of Contents

From the Article: "In the coming months, searching for supply chain talent, engaging in demand planning, and launching or fine-tuning sustainability initiatives will top the supply chain's to-do list."

Japan's Rapidus positioning to win 2nm chip race

Source: https://newyorkfolk.com/news/japans-rapidus-positioning-to-win-2nm-chip-race/

From the Article: "All of this is important to the success of Rapidus, which will progress towards 2nm with the support of the complete US, European and Japanese semiconductor ecosystems."

Designing and securing chips for outer space

Source: https://semiengineering.com/designing-and-securing-chips-for-outer-space/

From the Article: "Utilizing what's learned in automotive designs to make devices in space more reliable."

Applied Materials to open S$600 million factory in Singapore, doubling manuf - Techgoondu

Source: https://www.techgoondu.com/2022/12/22/applied-materials-to-open-s600-million-factory-in-singapore-doubling-manuf/

From the Article: "Semiconductor equipment maker Applied Materials is set to open a S$600 million factory in Singapore in 2024 that will double its manufacturing footprint in the country."

The Right Time For Chip Export Controls

Source: https://www.lawfareblog.com/right-time-chip-export-controls

From the Article: "BIS explained that the export controls were imposed to restrict China's ability "to produce advanced military systems including weapons of mass destruction; improve the speed and accuracy of its military decision making, planning,

and logistics, as well as of its autonomous military systems; and commit human rights abuses.”"

A Look Ahead: 2023 Connectivity Trends for Smart Manufacturing

Source: https://www.industryweek.com/technology-and-iiot/article/21256000/a-look-ahead-2023-connectivity-trends-for-smart-manufacturing

From the Article: "Out of sheer necessity, 2022 became the year of digital transformation. Manufacturing executives were forced to adapt, and adapt they have. We’ve seen innovation at every level of the pipeline and priorities set to streamline operations and increase agility.”

China's YMTC faces NAND production issues after US blacklist

Source: https://www.theregister.com/2022/12/18/us_blacklist_spells_trouble/

From the Article: "One research firm thinks YMTC may have to exit 3D NAND altogether"

SEMI: global semiconductor industry invests $500 billion to build 84 new fabs by 2024

Source: https://www.digitimes.com/news/a20221213VL201/semi-semiconductor-industry.html

From the Article: "Semiconductor Equipment Manufacturers International (SEMI) released its latest World Fab Forecast report, projecting the worldwide semiconductor industry will invest more than $500 billion in 84 volume chipmaking facilities by 2024."

Bringing economics back into EU and U.S. chips policy

Source: https://www.brookings.edu/techstream/bringing-economics-back-into-the-politics-of-the-eu-and-u-s-chips-acts-china-semiconductor-competition/

From the Article: "Along with unprecedented restrictions on semiconductor components, the rhetoric and regulations coming out of the U.S. and Europe gesture toward a reversal of a decades-long trend of globalization and raise an important set of policy

questions: why have the U.S. and EU been looking to reshore industries?"

Samsung transfers US patents to Huawei

Source: http://thelec.net/news/articleView.html?idxno=4327

From the Article: "Samsung transferred 98 patents it has in the US to Huawei last month, TheElec has learned. Combined with the 81 patents it handed over in 2019 to the Chinese company the Korean firm has given Huawei 179 patents in total so far."

Gallium oxide a new generation of semiconductor material for power devices

Source: https://www.powerelectronicsnews.com/gallium-oxide-a-new-generation-of-semiconductor-material-for-power-devices/

From the Article: "Research has come up with an ultra-WBG material, β-Gallium oxide—β-Ga2O3, which improves the overall performance of power electronic devices."

Semi taiwan launches rating service to strengthen cybersecurity across taiwan chip ecosystem

Source: https://www.semi.org/en/news-media-press-releases/semi-press-releases/semi-taiwan-launches-rating-service-to-strengthen-cybersecurity-across-taiwan-chip-ecosystem

From the Article: "HSINCHU, Taiwan – December 13, 2022 – Taking aim at hardening the Taiwan semiconductor ecosystem's defenses against cyberattacks, SEMI has launched a Semiconductor Cybersecurity Risk Rating Service. Using third-party risk scoring and risk posture assessment, the service is designed to help SEMI Taiwan members assess cybersecurity risks in real time and provide risk remediation guidance."

Chen named director of Purdue's Birck Nanotechnology Center - Research at Purdue

Source: https://www.purdue.edu/research/features/stories/chen-named-director-of-purdues-birck-nanotechnology-center/

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

From the Article: "WEST LAFAYETTE, Ind. – Recognized worldwide for two decades of excellence in nanotechnology research, Zhihong Chen has been named the Mary Jo and Robert L. Kirk Director of the Birck Nanotechnology Center after serving one year as the center's interim director. Her directorship becomes effective Jan. 1."

Intel splits graphic chips unit two

Source: https://www.businesstimes.com.sg/companies-markets/intel-splits-graphic-chips-unit-two

From the Article: "INTEL is splitting its graphic chips unit into two, the company said on Wednesday (Dec 21), as it realigns the business to better compete with Nvidia and Advanced Micro Devices (AMD)."

Samsung makes the world's first DDR5 DRAM chips using 12nm tech

Source: https://www.sammobile.com/news/samsung-makes-worlds-first-ddr5-dram-chips-12nm-tech/

From the Article: "Samsung has unveiled the world's first DDR5 DRAM chips that are made using 12nm semiconductor fabrication technology. The company revealed its 16Gb DDR5 DRAM chips and said that they've already been evaluated for compatibility with AMD's Zen processors."

Semi europe and european commission representatives develop key actions to tackle chip industry skills shortage

Source: https://prod8.semi.org/en/news-media-press-releases/semi-press-releases/semi-europe-and-european-commission-representatives-develop-key-actions-to-tackle-chip-industry-skills-shortage

From the Article: "BRUSSELS, Belgium — December 19, 2022 — SEMI, the industry association serving the global electronics design and manufacturing supply chain, today announced key actions proposed by SEMI Europe and European Commission (EC) representatives in consultation with semiconductor industry stakeholders to overcome the skills shortage in Europe's microelectronics industry."

Link back to Table of Contents

SemiconX:-AI Acceleration Hardware

Source: https://medium.com/@ghota/semiconx-ai-acceleration-hardware-3bc18738132f

From the Article: "Artificial Intelligence (AI) is a powerful tool that will be ubiquitous in the upcoming decade, in applications spanning across defense, automobiles, robotics, healthcare, metaverse, and industry 4.0."

€1.7m for semiconductor tech in new public/private project

Source: https://delano.lu/article/1-7m-for-semiconductor-chip-te

From the Article: "A new project between Rotarex and LIST seeks to improve the process of making semiconductor chips, benefiting both the private company and the public institution."

Samsung Electronics Develops Industry's First 12nm-Class DDR5 DRAM

Source: https://news.samsung.com/global/samsung-electronics-develops-industrys-first-12nm-class-ddr5-dram

From the Article: "Set to begin mass production in 2023, Samsung's new DRAM will advance next-generation computing, data centers and AI applications with industry-leading performance and greater power efficiency"

SIA Applauds Increased Funding for Research, Workforce Development in Year-End Funding Package

Source: https://www.semiconductors.org/sia-applauds-increased-funding-for-research-workforce-development-in-year-end-funding-package/

From the Article: ""“Building off the important investments made by the CHIPS and Science Act, SIA applauds increased funding for research and workforce development in the FY2023 Omnibus."

IEDM 2022: Did We Just Witness The Death Of SRAM?

Link back to Table of Contents

Source: https://fuse.wikichip.org/news/7343/iedm-2022-did-we-just-witness-the-death-of-sram/

From the Article: "While there were a great number of interesting papers from both academia and industry, it was the one by TSMC that brought frighteningly bad news – whereas logic is still scaling more-or-less along the historical trendline, SRAM scaling appears to have completely collapsed."

German firms splash out billions in Taiwan trade for 'stable supply chain'

Source: https://www.scmp.com/economy/china-economy/article/3203863/german-firms-splash-out-billions-taiwan-supply-chain-largely-semiconductors-and-chemicals

From the Article: "Sustainable and reliable business-to-business exchanges have been cultivated between Taiwan and Germany during the pandemic, and trade keeps widening. With the global economy in flux, 'quicker and more intensive' talks have also been taking place between German and Taiwanese firms in the realm of renewable energy"

Sonic lift off tech aims to reduce semiconductor costs

Source: https://www.eetimes.com/sonic-lift-off-tech-aims-to-reduce-semiconductor-costs/

From the Article: "Semiconductor device manufacturing requires the availability of high-quality wafers with perfectly flat and smooth surfaces. The quality of a wafer's surface is fundamental to ensuring high-performing and reliable devices."

What TSMC CEO CC Wei says about the semiconductor industry (1)

Source: https://www.digitimes.com/news/a20221221VL201/semiconductor-tsmc.html&chid=12

From the Article: "With the presidents of three major universities in the audience, Wei said that we have to trust the government on land and power issues, but how to get the most talent will be the biggest challenge for TSMC. He hopes that the local universities will produce more graduates that TSMC can hire, and that the clients in the audience will give his company more orders."

Link back to Table of Contents

TSMC's CEO is not pleased with the growing US-China rift

Source: https://www.theregister.com/2022/12/21/tsmcs_ceo_us_china/

From the Article: " Leader of the the world's largest contract chip manufacturer would like it if the two world powers could work out their differences"

Evertiq - Fujifilm expands with new semiconductor materials facility

Source: https://evertiq.com/design/53036

From the Article: "Fujifilm says it plans to build a new advanced semiconductor materials manufacturing facility in South Korea as it looks to further expand the electronic materials business."

India and Vietnam could benefit as chipmakers shift away from China

Source: https://www.cnbc.com/2022/12/13/india-vietnam-may-benefit-as-chipmakers-shift-from-china-amid-us-curbs.html

From the Article: "The Biden administration's China chip curbs are the latest in a series of upheavals prompting chipmakers to relocate production chains to neighboring countries, experts say. Among them, Vietnam and India have emerged as cost-efficient alternative bases with lower levels of political risks. Still, experts say China continues to maintain a comfortable lead in chipmaking prowess over emerging hubs."

Study identifies most likely locations for semiconductor plants in US

Source: https://techxplore.com/news/2022-12-semiconductor.html

From the Article: "With the likelihood of the U.S. experiencing growth in the manufacturing of semiconductors, researchers at Ball State University have pinpointed the locations across the country most likely to experience expansion of semiconductor chip production in the coming years."

Link back to Table of Contents

Pragmatic semiconductor boosts series c funding 125m

Source: https://www.businessweekly.co.uk/news/hi-tech/pragmatic-semiconductor-boosts-series-c-funding-125m

From the Article: "PragmatIC Semiconductor, a Cambridge-based world leader in flexible electronics, has secured $35 million additional investment from high quality institutional investors – including a US intelligence community influencer. "

TSMC fends off Samsung to secure huge 4nm chip order from Tesla

Source: https://www.androidheadlines.com/2022/12/tsmc-fends-off-samsung-to-secure-huge-4nm-chip-order-from-tesla.html

From the Article: "Tesla has chosen TSMC as the chip supplier for its future self-driving cars. The Elon Musk-led EV (electric vehicle) company will obtain 4nm chips from TSMC's new semiconductor factory in Arizona, US. The Taiwanese semiconductor giant fended off competition from Samsung to secure this massive order."

Two thyssenkrupp divisions targeted in cyberattack, though no data breached - Industrial Cyber

Source: https://industrialcyber.co/news/two-thyssenkrupp-divisions-targeted-in-cyberattack-though-no-data-breached/

From the Article: "Industrial engineering and steel production conglomerate thyssenkrupp AG confirmed that it was fending off a cyberattack against two of its divisions, though no data appeared to have been compromised."

Inside Joe Biden's battle to destroy the Chinese microchip industry

Source: https://www.telegraph.co.uk/business/2022/12/22/inside-joe-bidens-battle-destroy-chinese-microchip-industry/

From the Article: "The heavy codependency of the chip industry is now being weaponized by the Biden administration to slow China's rise"

Link back to Table of Contents

Top 7 factors boosting enterprise cybersecurity resilience - Help Net Security

Source: https://www.helpnetsecurity.com/2022/12/07/factors-cybersecurity-resilience/

From the Article: "Cybersecurity resilience has emerged as a top priority as a staggering 62 percent of organizations surveyed said they had experienced a security event that impacted business in the past two years."

Evelyn Wang appointed as director of US Department of Energy's Advanced Research Projects Agency-Energy

Source: https://news.mit.edu/2022/evelyn-wang-appointed-director-department-energy-arpa-e-1222

From the Article: "The head of MIT's Department of Mechanical Engineering was nominated by President Biden to lead ARPA-E's mission to support critical energy research."

Amazon helped rescue the Ukrainian government and economy using suitcase-sized hard drives brought in over the Polish border: 'You can't take out the cloud with a cruise missile'

Source: https://www.businessinsider.com/amazon-saved-the-ukrainian-government-with-suitcase-sized-hard-drives-2022-12

From the Article: "Amazon has been supporting Ukraine since the country was invaded by Russia in February. In one initiative, Amazon sent suitcase-sized computer drives to back up critical data to the cloud. 10 million gigabytes of Ukrainian government and economic data have been saved so far. "

Hackers Breach Okta's GitHub Repositories, Steal Source Code

Source: https://thehackernews.com/2022/12/hackers-breach-oktas-github.html

From the Article: "Okta, a company that provides identity and access management services, disclosed on Wednesday that some of its source code repositories were accessed in an unauthorized manner earlier this month."

Link back to Table of Contents

Over 16 lakh cyber crime incidents reported since 2020, says govt

Source: https://economictimes.indiatimes.com/tech/tech-bytes/over-16-lakh-cyber-crime-incidents-reported-since-2020-says-govt/articleshow/96198446.cms

From the Article: "Over 16 lakh cybercrime incidents have been reported in the country in the last three years following which more than 32,000 FIRs were registered, Lok Sabha was informed on Tuesday. "

SK Group chairman: Chip market's downturn will continue, but not for long

Source: https://m.koreaherald.com/view.php?ud=20221222000673

From the Article: "SK Group Chairman Chey Tae-won painted a gloomy outlook for the semiconductors industry, but predicted the downturn will not last long, as chip cycles have tended to grow shorter."

Supply Chain - Mexico's nearshoring potential: Weighing opportunities and risks

Source: https://library.gtxcel.com/supplychain/library/item/q3_2022/4050943/

From the Article: "MEXICO IS WELL PLACED to benefit from companies looking to nearshore, or relocate their operations closer to their main destination markets, in response to recent supply chain shocks such as the Russia-Ukraine conflict and China's dynamic COVID containment policy."

Flashpoint Year In Review: 2022 Financial Threat Landscape

Source: https://flashpoint.io/blog/risk-intelligence-year-in-review-financial/

From the Article: "This blog is part of our 2022 Year In Review, an intelligence retrospective highlighting the most significant trends of the past year—plus insight into 2023."

Insiders worry CISA is too distracted from critical cyber mission

Source: https://www.cyberscoop.com/cisa-dhs-easterly-cyber-mission/

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

From the Article: "But four years in, CISA appears to be struggling with internal divisions over the direction of the agency, morale problems and growing concerns about leadership priorities."

Cisco Bets on Quantum Key Distribution

Source: https://www.sdxcentral.com/articles/interview/cisco-bets-on-quantum-key-distribution/2022/12/

From the Article: "Cisco Chief Strategy Officer Liz Centoni expects quantum key distribution (QKD) to gain momentum next year as organizations and governments try to address post-quantum security threats."

Heap-based buffer overflow vulnerability in Fortinet FortiOS SSL-VPN appliances, patches available - Industrial Cyber

Source: https://industrialcyber.co/vulnerabilities/heap-based-buffer-overflow-vulnerability-in-fortinet-fortios-ssl-vpn-appliances-patches-available/?

From the Article: "Fortinet announced Monday that the presence of a heap-based buffer overflow vulnerability [CWE-122] in FortiOS SSL-VPN may allow a remote unauthenticated attacker to execute arbitrary code or commands via specifically crafted requests."

Facebook parent Meta agrees to pay $725 million to settle privacy lawsuit

Source: https://www.cnbc.com/2022/12/23/facebook-parent-meta-agrees-to-pay-725-million-to-settle-privacy-lawsuit-prompted-by-cambridge-analytica-scandal.html

From the Article: "Facebook parent Meta has agreed to pay $725 million to settle a class action lawsuit that claimed the social media giant gave third parties access to user data without their consent."

TikTok confirms that journalists' data was accessed by employees of its parent company | CNN Business

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Source: https://www.cnn.com/2022/12/22/tech/tiktok-bytedance-journalist-data/index.html

From the Article: "TikTok parent company ByteDance has fired four employees who improperly accessed the personal data of two journalists on the platform, TikTok spokesperson Brooke Oberwetter confirmed to CNN Thursday."

Taxonomy of Attacks on Open-Source Software Supply Chains

Source: https://arxiv.org/abs/2204.04008

From the Article: "The widespread dependency on open-source software makes it a fruitful target for malicious actors, as demonstrated by recurring attacks. The complexity of today's open-source supply chains results in a significant attack surface, giving attackers numerous opportunities to reach the goal of injecting malicious code into open-source artifacts that is then downloaded and executed by victims."

FrodoPIR: New Privacy-Focused Database Querying System

Source: https://thehackernews.com/2022/12/frodopir-new-privacy-focused-database.html

From the Article: "The developers behind the Brave open-source web browser have revealed a new privacy-preserving data querying and retrieval system called FrodoPIR."

Global semiconductor industry outlook for 2023

Source: https://advisory.kpmg.us/articles/2022/global-semiconductor-industry-outlook-2023.html

From the Article: "KPMG LLP and the Global Semiconductor Alliance (GSA) conducted the 18th annual global semiconductor industry survey in the fourth quarter of 2022. The survey captures insights from 151 semiconductor executives about their outlook for the industry in 2023 and beyond. "

CNBC|SurveyMonkey Small Business Index Q4 2022 | SurveyMonkey

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Source: https://www.surveymonkey.com/curiosity/cnbc-small-business-q4-2022/

From the Article: "Just 37% of small business owners are concerned that their business will be the victim of a cyber attack in the next 12 months, roughly consistent with the past three quarters."

Why state governments are banning TikTok

Source: https://thehill.com/homenews/nexstar_media_wire/3773798-why-state-governments-are-banning-tiktok/

From the Article: "At least half a dozen states have recently enacted bans on the use of TikTok by state employees and now some federal lawmakers are hoping to ban it nationwide. But why?"

Okta's source code stolen after GitHub repositories hacked

Source: https://www.bleepingcomputer.com/news/security/oktas-source-code-stolen-after-github-repositories-hacked/

From the Article: "Okta, a leading provider of authentication services and Identity and Access Management (IAM) solutions, says that its private GitHub repositories were hacked this month."

Vice Society Ransomware Attackers Adopt Robust Encryption Methods

Source: https://thehackernews.com/2022/12/vice-society-ransomware-attackers-adopt.html

From the Article: "The Vice Society ransomware actors have switched to yet another custom ransomware payload in their recent attacks aimed at a variety of sectors."

France Fines Microsoft €60 Million for Using Advertising Cookies Without User Consent

Source: https://thehackernews.com/2022/12/france-fines-microsoft-60-million-for.html

From the Article: "France's privacy watchdog has imposed a €60 million ($63.88 million)

Link back to Table of Contents

fine against Microsoft's Ireland subsidiary for dropping advertising cookies in users' computers without their explicit consent in violation of data protection laws in the European Union."

'Just in time' and 'just in case' systems leave retailers with too much inventory - RetailWire

Source: https://retailwire.com/discussion/just-in-time-and-just-in-case-systems-leave-retailers-with-too-much-inventory/

From the Article: ""“Just in case” thinking was supposed to prevent inventory outages and shortages. That seemed to have backfired. Retailers were announcing over-stocked positions starting in late spring and have been trying to promote their way out of the problem ever since. It’s unclear as we sit here in mid-December whether or not it’s working."

Malicious Python Trojan Impersonates SentinelOne Security Client

Source: https://www.darkreading.com/vulnerabilities-threats/malicious-python-trojan-impersonates-sentinelone-security-client

From the Article: "A fully functional SentinelOne client is actually a Trojan horse that hides malicious code within; it was found lurking in the Python Package Index repository ecosystem."

Living Security and GuidePoint Security collaborate to minimize human risk exposure

Source: https://www.helpnetsecurity.com/2022/12/15/living-security-guidepoint-security/

From the Article: "Living Security and GuidePoint Security collaboration will deliver Living Security’s Human Risk Management solutions and security awareness training to even more organizations within GuidePoint Security’s ecosystem."

Critical Windows code-execution vulnerability went undetected until now

Source: https://news.hitb.org/content/critical-windows-code-execution-vulnerability-went-undetected-until-now

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

From the Article: "Researchers recently discovered a Windows code-execution vulnerability that has the potential to rival EternalBlue, the name of a different Windows security flaw used to detonate WannaCry, the ransomware that shut down computer networks across the world in 2017."

Serious Linux kernel security hole uncovered

Source: https://news.hitb.org/content/serious-linux-kernel-security-hole-uncovered

From the Article: "The remote code execution (RCE) flaw allowed unauthenticated users to execute kernel-level code and received the maximum possible severity rating on the common vulnerability reporting system (CVSS)."

Hands On With Flipper Zero, the Hacker Tool Blowing Up on TikTok

Source: https://news.hitb.org/content/hands-flipper-zero-hacker-tool-blowing-tiktok

From the Article: "Across the US, countless buildings, from government offices to your next hotel room door, are protected by RFID-controlled locks. On a recent trip to my office, I passed nearly 20 of these keyless entry systems, which are among the most pervasive in the world."

Microsoft discovers Windows/Linux botnet used in DDoS attacks

Source: https://news.hitb.org/content/microsoft-discovers-windowslinux-botnet-used-ddos-attacks

From the Article: "Microsoft researchers have discovered a hybrid Windows-Linux botnet that uses a highly efficient technique to take down Minecraft servers and performs distributed denial-of-service attacks on other platforms."

Buyer Beware! Account Takeover Attacks Surging This Shopping Season

Source: https://www.imperva.com/blog/buyer-beware-account-takeover-attacks-surging-this-shopping-season/

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

From the Article: "The prevalence of Account Takeover (ATO) attacks continues to rise, as the threat creeps its way to the top of the list of security concerns for organizations today. Last year, Imperva recorded a staggering 148% increase in Account Takeover attacks, as reported in the 2022 Bad Bot Report."

The World Cup: Prime Time for Sports Fans and Cybercriminals

Source: https://www.imperva.com/blog/the-world-cup-prime-time-for-sports-fans-and-cybercriminals/

From the Article: "From November 20 to December 18, fans from all over the world are tuned into the World Cup tournament in Qatar. While this is a major event for sports fans, it's also prime time for bad actors."

Chinese state-sponsored hacker group RedDelta targeting organizations within Europe, Southeast Asia

Source: https://industrialcyber.co/ransomware/chinese-state-sponsored-hacker-group-reddelta-targeting-organizations-within-europe-southeast-asia/

From the Article: "Cybersecurity firm Recorded Future's Insikt Group continues to track activity attributed to the likely Chinese state-sponsored threat activity group RedDelta targeting organizations within Europe and Southeast Asia using a customized variant of the PlugX backdoor."

SentinelLabs details Vice Society ransomware group using custom-branded ransomware payload

Source: https://industrialcyber.co/ransomware/sentinellabs-details-vice-society-ransomware-group-using-custom-branded-ransomware-payload/

From the Article: "SentinelLabs disclosed that the Vice Society group has adopted a new custom-branded ransomware payload in recent intrusions, dubbed 'PolyVice,' which implements an encryption scheme, using NTRUEncrypt and ChaCha20-Poly1305 algorithms."

Two thyssenkrupp divisions targeted in cyberattack, though no data breached

Link back to Table of Contents

Source: https://industrialcyber.co/news/two-thyssenkrupp-divisions-targeted-in-cyberattack-though-no-data-breached/

From the Article: "Industrial engineering and steel production conglomerate thyssenkrupp AG confirmed that it was fending off a cyberattack against two of its divisions, though no data appeared to have been compromised."

NSA report focuses on driving cybersecurity outcomes while pushing strong partnerships and education

Source: https://industrialcyber.co/reports/nsa-report-focuses-on-driving-cybersecurity-outcomes-while-pushing-strong-partnerships-and-education/

From the Article: "The National Security Agency (NSA) has released its 2022 Cybersecurity Year in Review highlighting the agency's ability to scale cybersecurity solutions through strong partnerships, resulting in speed and agility."

Evolving cyber threats push organizations to chalk out improved incident response, business continuity, disaster recovery plans

Source: https://industrialcyber.co/features/evolving-cyber-threats-push-organizations-to-chalk-out-improved-incident-response-business-continuity-disaster-recovery-plans/

From the Article: "With the growing threat of cybersecurity incidents targeting critical infrastructure installations, governments and organizations around the world are forced to roll out their best defense in a rapidly evolving cyber threat environment and work on building resilience."

Nozomi researchers track malicious Glupteba trojan activity through blockchain technology

Source: https://industrialcyber.co/vulnerabilities/nozomi-researchers-track-malicious-glupteba-trojan-activity-through-blockchain-technology/

From the Article: "Researchers from Nozomi Networks Labs announced Thursday that the Glupteba trojan is an example of a hacker leveraging blockchain-based technologies to carry out their malicious activity. The backdoor trojan is downloaded using 'Pay-Per-Install' networks – online ad campaigns that prompt software or application downloads – in infected installers or software cracks. "

Link back to Table of Contents

NSA warns of Chinese hacker group APT5 targeting Citrix ADC vulnerabilities

Source: https://industrialcyber.co/ransomware/nsa-warns-of-chinese-hacker-group-apt5-targeting-citrix-adc-vulnerabilities/

From the Article: "The National Security Agency (NSA) issued Tuesday a threat hunting guidance that provides steps for organizations to take in order to look for possible artifacts of Chinese hacker group APT5, which attacks Citrix Application Delivery Controller (ADC) vulnerabilities."

FBI: Cyber-Criminals Are Purchasing Search Engine Ad Services to Launch Attacks

Source: https://www.infosecurity-magazine.com/news/fbi-cyber-search-engine-ads-attacks/

From the Article: "The FBI warns that cyber-criminals are impersonating brands through purchasing ad services in order to lure users to malicious websites."

Researchers Develop AI-powered Malware Classification for 5G-enabled IIoT

Source: https://www.infosecurity-magazine.com/news/ai-malware-classification-for-5g/

From the Article: "A team of researchers came up with an ingenuous method leveraging AI to detect and classify malware in IIoT devices."

Cyber-Incident Causes System Failures at Canadian Children's Hospital

Source: https://www.infosecurity-magazine.com/news/cyber-incident-failure-children/

From the Article: "The ongoing incident has impacted clinical and corporate systems, as well as some hospital phone lines and webpages."

US Most Impacted by Data Breaches in the Financial Industry in 2022

Source: https://www.infosecurity-magazine.com/news/us-most-impacted-data-breaches/

Link back to Table of Contents

The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

From the Article: "While 57% of these breaches were attributed to different types of malware, ATM skimming still accounted for 6.5% of all attacks targeting the financial sector."

UK Security Agency Wants Fresh Approach to Combat Phishing

Source: https://www.infosecurity-magazine.com/news/uk-security-agency-combat-phishing/

From the Article: "NCSC says "blame and fear" won't work."

Organizations Warned of New Attack Vector in Amazon Web Services

Source: https://www.infosecurity-magazine.com/news/warned-attack-vector-amazon-web/

From the Article: "Researchers warned that threat actors could potentially exploit Elastic IP transfer and compromise an IP address."

Ukraine's Delta Military Intel System Hit by Attacks

Source: https://www.infosecurity-magazine.com/news/ukraines-delta-military-intel/

From the Article: "Phishing campaign spotted by CERT-UA."

Ransomware Groups to Increase Zero-Day Exploit-Based Access Methods in the Future

Source: https://www.infosecurity-magazine.com/news/ransomware-groups-increase-zeroday/

From the Article: "Trend Micro's latest research paper analyzed ways in which ransomware groups could evolve to stay on top of strengthened cyber-protection measures."

Agenda Ransomware Switches to Rust to Attack Critical Infrastructure

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Source: https://www.infosecurity-magazine.com/news/agenda-ransomware-switch-to-rust/

From the Article: "Victim companies have a combined revenue of around $550m."

Social Blade Confirms Data Breach Exposing PII on the Dark Web

Source: https://www.infosecurity-magazine.com/news/social-blade-confirms-data-breach/

From the Article: "The company confirmed the data does not include any credit card information."

Aussie Data Breaches Surge 489% in Q4 2022

Source: https://www.infosecurity-magazine.com/news/aussie-data-breaches-surge-489-q4/

From the Article: "Country bucks the global trend thanks to high-profile incidents."

Multiple vulnerabilities in Trend Micro Apex One and Apex One as a Service

Source: https://jvn.jp/en/vu/JVNVU96679793/

From the Article: "Trend Micro Incorporated has released security updates for Apex One and Apex One as a Service."

Use-after-free vulnerability in Omron CX-Drive

Source: https://jvn.jp/en/vu/JVNVU92689335/

From the Article: "OMRON CX-Drive contains a use-after-free vulnerability."

Zenphoto vulnerable to cross-site scripting

Source: https://jvn.jp/en/jp/JVN06093462/

Link back to Table of Contents

The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

From the Article: "Zenphoto contains a cross-site scripting vulnerability."

Hacked Ring Cams Used to Record Swatting Victims

Source: https://krebsonsecurity.com/2022/12/hacked-ring-cams-used-to-record-swatting-victims/

From the Article: "Two U.S. men have been charged with hacking into the Ring home security cameras of a dozen random people and then “swatting” them — falsely reporting a violent incident at the target’s address to trick local police into responding with force."

Godfather Malware Makes Banking Apps An Offer They Can't Refuse

Source: https://www.theregister.com/2022/12/22/godfather_banking_trojan/

From the Article: "Crooks are using an Android banking Trojan dubbed Godfather to steal from banking and cryptocurrency exchange app users in 16 countries, according to Group-IB security researchers."

Godfather Android banking malware is on the rise

Source: https://www.malwarebytes.com/blog/news/2022/12/godfather-android-banking-malware-is-on-the-rise

From the Article: "The new version of Godfather uses an icon and name similar to a legitimate application named MYT Music, which is hosted on the Google Play Store with over 10 million downloads."

4 over-hyped security vulnerabilities of 2022

Source: https://www.malwarebytes.com/blog/news/2022/12/4-times-security-vulnerabilities-were-blown-out-of-proportion-in-2022

From the Article: "A critical vulnerability can send countless organizations into chaos, as security teams read up on the vulnerability, try to figure out whether it applies to their

systems, download any potential patches, and deploy those fixes to affected machines."

Update now! Apple patches active exploit vulnerability for iPhones

Source: https://www.malwarebytes.com/blog/news/2022/12/update-now-apple-patches-active-exploit-vulnerability-for-iphones

From the Article: "Apple has released new security content for iOS 16.1.2 and Safari 16.2. Normally we would say that Apple pushed out updates, but in this mysterious case the advisory is about an iPhone software update Apple released two weeks ago. As it turns out, to fix a zero-day security vulnerability that was actively exploited."

Gatekeeper's Achilles heel: Unearthing a macOS vulnerability

Source: https://www.microsoft.com/en-us/security/blog/2022/12/19/gatekeepers-achilles-heel-unearthing-a-macos-vulnerability/

From the Article: "On July 27, 2022, Microsoft discovered a vulnerability in macOS that can allow attackers to bypass application execution restrictions imposed by Apple's Gatekeeper security mechanism, designed to ensure only trusted apps run on Mac devices."

S3 Ep114: Preventing cyberthreats – stop them before they stop you! [Audio + Text]

Source: https://nakedsecurity.sophos.com/2022/12/22/s3-ep114-preventing-cyberthreats-stop-them-before-they-stop-you-audio-text/

From the Article: "Join world-renowned expert Fraser Howard, Director of Research at SophosLabs, for this fascinating episode on how to fight cybercrime."

Patch Tuesday: 0-days, RCE bugs, and a curious tale of signed malware

Source: https://nakedsecurity.sophos.com/2022/12/14/patch-tuesday-0-days-rce-bugs-and-a-curious-tale-of-signed-malware/

From the Article: "Tales of derring-do in the cyberunderground! (And some zero-days.)"

Link back to Table of Contents

COVID-bit: the wireless spyware trick with an unfortunate name

Source: https://nakedsecurity.sophos.com/2022/12/13/covid-bit-the-wireless-spyware-trick-with-an-unfortunate-name/

From the Article: "It's not the switching that's the problem, it's the switching of the switching!"

Email Hijackers Scam Food Out Of Businesses, Not Just Money

Source: https://www.theregister.com/2022/12/17/in_brief_security/

From the Article: "Business email compromise (BEC) continues to be a multibillion-dollar threat, but it's evolving, with the FBI and other federal agencies warning that cybercriminals have started using spoofed emails to steal shipments of physical goods – in this case, food. "

Microsoft Discovers Windows / Linux Botnet Used In DDoS Attacks

Source: https://arstechnica.com/information-technology/2022/12/microsoft-discovers-windows-linux-botnet-used-in-ddos-attacks/

Brute Force Attacks: A Guide to Protecting Your Online Information

Source: https://www.pandasecurity.com/en/mediacenter/security/brute-force-attack/

From the Article: "A brute force attack is a hacking strategy in which a cybercriminal attempts to log into an account by trying multiple password options until successful. With the help of computer scripts, hackers can make thousands of attempts per second — hacking simple passwords in the blink of an eye."

What Is Whaling? Your Guide to Identifying and Preventing Whaling Phishing Attacks

Source: https://www.pandasecurity.com/en/mediacenter/security/whaling/

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

From the Article: "Have you ever received an email from a trusted sender who really turned out to be an online phisher? If so, you're not alone, and even large organizations like Snapchat and Seagate have fallen victim to whaling phishing attacks."

Beyond Ransomware: Cybercrime Trends to Watch in 2023

Source: https://www.dice.com/career-advice/beyond-ransomware-cybercrime-trends-to-watch-in-2023

From the Article: "The global cybercrime problem continues to grow and change, bringing with it additional challenges for those tech and cybersecurity pros entrusted with securing their organizations' data and infrastructure."

Expanded attacks launched by Iranian threat operation

Source: https://www.scmagazine.com/brief/critical-infrastructure/expanded-attacks-launched-by-iranian-threat-operation

From the Article: "Iranian hacking operation Charming Kitten, also known as TA453, APT42, and Phosphorous, has expanded its operations to target critical infrastructure, medical researchers, and U.S. politicians, CyberScoop reports."

Implement Risk-Based Vulnerability Management with Qualys TruRisk™ : Part 2

Source: https://blog.qualys.com/vulnerabilities-threat-research/2022/12/16/implement-risk-based-vulnerability-management-with-qualys-trurisk-part-2

From the Article: "This blog is a continuation of our first blog on implementing risk-based vulnerability management with Qualys TruRiskTM. In the first blog, we covered how to correctly tag and categorize assets for accurate risk assessment. "

New info-stealer malware infects software pirates via fake cracks sites - Bleeping Computer

Source: https://www.bleepingcomputer.com/news/security/new-info-stealer-malware-infects-software-pirates-via-fake-cracks-sites/

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

From the Article: "A new information-stealing malware named ‘RisePro’ is being distributed through fake cracks sites operated by the PrivateLoader pay-per-install (PPI) malware distribution service."

Your business should compensate for modern ransomware capabilities right now

Source: https://venturebeat.com/security/your-business-should-compensate-for-modern-ransomware-capabilities-right-now/

From the Article: "The “if, not when” mentality surrounding ransomware may be the biggest modern threat to business longevity. Companies of all sizes and across all industries are increasingly common targets for ransomware attacks, and we know that 94% of organizations experienced a cybersecurity incident last year alone. "

Queensland University of Technology hit by Ransomware - IT Security News

Source: https://www.itsecuritynews.info/queensland-university-of-technology-hit-by-ransomware/

From the Article: "A ransomware hit Queensland University of Technology (QUT) in the early hours of today, crippling a portion of the institute’s network from the past 5 hours. The second largest University seems to have been hit badly as whole of the printers operating in the campus are displaying the ransomware note."

Under cyber attack: The AIIMS ransomware attack is just a reminder how vulnerable ...

Source: https://www.financialexpress.com/life/technology-under-cyber-attack-the-aiims-ransomware-attack-is-just-a-reminder-how-vulnerable-organisations-can-be-2925514/

From the Article: "Cybercrimes are rising both in numbers and sophistication. The latest to find itself on the receiving end was the All India Institute of Medical Sciences (AIIMS) in Delhi, which was hit by a ransomware attack on November 23, rendering its servers non-functional for about two weeks."

Answering a call or going to the start of the cell phone downloads malware that steals data

Link back to Table of Contents

Source: https://thetimeshub.in/answering-a-call-or-going-to-the-start-of-the-cell-phone-downloads-malware-that-steals-data/3417/

From the Article: "A new case of ransomware on Android was released by the Microsoft cybersecurity team, it is a virus that attacks the cell phone by turning off the screen for the user to press the start button and proceed to the hack, in fact, it was also identified that it can be activated when answering a call."

The Dangers of Discord: What Is a Discord Virus? - MakeUseOf

Source: https://www.makeuseof.com/what-is-discord-virus/

From the Article: "Discord is a popular VoIP (voice over IP) and chat app for gamers that has taken the world by storm. While it is a great app for staying in touch with friends and gaming partners, there are some dangers that come with using Discord."

The age-old question in 2023: How to deal with ransomware? - BetaNews

Source: https://betanews.com/2022/12/24/2023-how-to-deal-with-ransomware/

From the Article: "It has been a devastating year for organizations in the fight against ransomware, with the news this year being a revolving door of ransomware breaches. Research by Zscaler revealed that there had been an 80 percent increase in ransomware attacks year-over-year."

Xavier University Might Have Lost Personal Data in Hack - Government Technology

Source: https://www.govtech.com/education/higher-ed/xavier-university-might-have-lost-personal-data-in-hack

From the Article: " Xavier University's computer network was hit by a cyberattack last month, potentially compromising students and employees' personal information, according to an email sent Thursday to students and staff."

Global counter-ransomware task force to become active in January - CyberScoop

Source: https://www.cyberscoop.com/ransomware-australia-task-force/

Link back to Table of Contents

From the Article: "Clare O'Neil, the Australian cybersecurity minister, plans to announce in coming days that a global task force to counter ransomware will become operational next month, the latest step in a global effort that began in Washington to fight back against the growing number of cyberattacks, a senior Biden administration official told CyberScoop."

Top 10 Risks in Cyber Security

Source: https://securityboulevard.com/2022/12/top-10-risks-in-cyber-security/

From the Article: "Increasing cyber security threats continue creating problems for companies and organizations, obliging them to defend their systems against cyber threats. According to research conducted by PurpleSec, the annual cost of cybercrime has risen to $6 trillion. In fact, 66% of companies have experienced cyber-attacks in the past 12 months."

Protecting your organization from rising software supply chain attacks | VentureBeat

Source: https://venturebeat.com/security/protecting-your-organization-from-rising-software-supply-chain-attacks/

From the Article: "Attackers find it hard to resist the lure of software supply chains: They can all-too quickly and easily access a wide breadth of sensitive information — and thus gain juicier payouts. "

Vice Society Ransomware Attackers Adopt Robust Encryption Methods - The Hacker News

Source: https://thehackernews.com/2022/12/vice-society-ransomware-attackers-adopt.html

From the Article: "The Vice Society ransomware actors have switched to yet another custom ransomware payload in their recent attacks aimed at a variety of sectors."

Fool Me Thrice? How to Avoid Double and Triple Ransomware Extortion - Dark Reading

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Source: https://www.darkreading.com/vulnerabilities-threats/fool-me-thrice-how-to-avoid-double-and-triple-ransomware-extortion-

From the Article: "The danger of being hit by a ransomware attack is scary enough, but in many cases, criminals can still extort your business after the ransom has been paid and things have seemingly returned to normal."

The Week in Ransomware - December 23rd 2022 - Targeting Microsoft Exchange

Source: https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-december-23rd-2022-targeting-microsoft-exchange/

From the Article: "Reports this week illustrate how threat actors consider Microsoft Exchange as a prime target for gaining initial access to corporate networks to steal data and deploy ransomware."

Ransomware In-Advance Prevention Storage is Released, Not a Backup Storage - Benzinga

Source: https://www.benzinga.com/pressreleases/22/12/g30185979/ransomware-in-advance-prevention-storage-is-released-not-a-backup-storage

From the Article: "Today more ransomware is targeting small and medium-sized businesses and hospitals without having enough resources and IT manpower. Backup is the only solution, but even that is not well-kept."

The Good, the Bad and the Ugly in Cybersecurity - Week 52 - SentinelOne

Source: https://www.sentinelone.com/blog/the-good-the-bad-and-the-ugly-in-cybersecurity-week-52-3/

From the Article: "CNIL hit Google and Meta with $68 million and $170 million fines respectively earlier this year for failing to offer users of their products transparent ways to reject tracking cookies."

Putin Team ransomware emerges from leaked Conti's source code - Cybernews

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Source: https://cybernews.com/news/putin-team-ransomware-emerges-from-leaked-contis-source-code/

From the Article: "Putin Team ransomware has likely emerged from the altered Conti's code. The group claims to be of Russian origin, although, according to CRIL, there is no evidence to support this. Threat actors utilize Telegram to share information about their victims, disclosing two victims thus far."

Paying ransomware is financing crime — how organizations can break the cycle | BetaNews

Source: https://betanews.com/2022/12/23/paying-ransomware-is-financing-crime-how-organizations-can-break-the-cycle/

From the Article: "Ransomware attacks have dominated the headlines over the last two years and will continue to control the cybersecurity agenda going into 2023. While ransomware gangs continue to be successful in extorting money from businesses, those that do pay demands are financing the ransomware industry and further crime."

Ransomware Is on the Rise—Here's How to Protect Yourself - PCMag UK

Source: https://uk.pcmag.com/ransomware-protection/144563/ransomware-is-on-the-rise-heres-how-to-protect-yourself

From the Article: "Today's ransom notes rarely appear in physical mailboxes with type cut from magazines. Instead, they often take the form of ransomware, or a type of malware that threatens to take action against a victim—often, blocking access to a key platform, website, or service via encryption—until a ransom is paid."

Wallix partners 3DS Outscale to strengthen cybersecurity - SecurityBrief Asia

Source: https://securitybrief.asia/story/wallix-partners-3ds-outscale-to-strengthen-cybersecurity

From the Article: "Wallix, an access and identity solutions provider recognised as a leader by the analyst firms Gartner, KuppingerCole, Quadrant Knowledge Solutions and Frost and Sullivan, has joined forces with hyper-trust cloud 3DS Outscale to strengthen its cybersecurity offering."

Link back to Table of Contents

Conti ransomware captures Costa Rica, Musk makes Twitter bid – April 2022 in review

Source: https://techmonitor.ai/technology/cybersecurity/musk-twitter-conti-ransomware-costa-rica-pegasus-spyware

From the Article: "Seeing businesses disrupted by ransomware gangs is nothing new, but in April notorious Russian hackers Conti went a step further and held the nation of Costa Rica to ransom."

Ransomware Payouts Declined in 2022: Crystal Blockchain - Globe Echo

Source: https://globeecho.com/business/crypto/ransomware-payouts-declined-in-2022-crystal-blockchain/

From the Article: "Victims of ransomware attacks paid hackers 4.5 times less in crypto in 2022 than in 2021, according to a new report."

Tesla's Chinese rival falls victim to bitcoin ransomware attack - Royals Blue

Source: https://www.royalsblue.com/teslas-chinese-rival-falls-victim-to-bitcoin-ransomware-attack/

From the Article: "Ransomware is a type of malware that takes control of a computer and blocks access to data until a ransom is paid."

Breaking News: Toronto children's hospital confirms it was hit by ransomware

Source: https://www.itworldcanada.com/article/breaking-news-toronto-childrens-hospital-confirms-it-was-hit-by-ransomware/519357

From the Article: "In an online statement today the hospital said it anticipates that it will be a matter of weeks before all systems are functioning as normal. There is no evidence to date that personal information or personal health information has been impacted."

Top 10 cyber crime stories of 2022 - Computer Weekly

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Source: https://www.computerweekly.com/news/252528238/Top-10-cyber-crime-stories-of-2022

From the Article: "High-profile cyber attacks elevated cyber security and cyber crime to dinner table conversation in 2021, and although there was no repeat of the Colonial Pipeline incident in 2022, awareness of cyber issues among the general public has never been higher."

As Ransomware Attacks Increase, EnduraData Announces Solutions - Newstrail.com

Source: https://www.newstrail.com/as-ransomware-attacks-increase-enduradata-announces-solutions/

From the Article: "According to Cybersecurity Ventures, Ransomware will have an annual global impact of $265 billion by 2031, with new attacks on consumers and businesses occuring every two seconds."

Defence body warns of data breaches and ransomware attacks, advises staff to follow CERT ...

Source: https://www.moneycontrol.com/news/business/defence-body-warns-of-data-breaches-and-ransomware-attacks-advises-staff-to-follow-cert-in-guidelines-9745741.html

From the Article: "The Controller General of Defence Accounts (CGDA), which oversees the Defence Accounts Department (DAD) in the Ministry of Defence, recently notified its employees of an increase in data breaches and data leaks from government offices and advised its staff to adhere to an advisory issued by the Indian Computer Emergency Response Team (CERT-In) in order to prevent such cyber threats."

Kaspersky uncovers attacks targeting Albanian government with ransomware and wipers ...

Source: https://financialpost.com/globe-newswire/kaspersky-uncovers-attacks-targeting-albanian-government-with-ransomware-and-wipers-signed-with-stolen-certificates

From the Article: " Kaspersky has shared its discovery of a malicious campaign aimed at Albanian government organizations, performed in two waves from July to September 2022."

Link back to Table of Contents

The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

After ransomware hits Colombian energy firm, Moody's says low patch rate suggests ...

Source: https://www.scmagazine.com/analysis/ransomware/after-ransomware-hits-colombian-energy-firm-moodys-says-low-patch-rate-suggests-inadequacies-in-cyber-practices

From the Article: "A ransomware attack at top Colombian energy company Empresas Publicas de Medellin (EPM) may damage its credit quality, setting an alarm clock for the critical infrastructure industry to develop efficient mitigation practices and vulnerability management programs, Moody's said. "

Vice Society ransomware gang is using a custom locker - Security Affairs

Source: https://securityaffairs.co/wordpress/139924/cyber-crime/vice-society-ransomware-custom-locker.html

From the Article: "SentinelOne researchers discovered that the Vice Society ransomware gang has started using a custom ransomware that implements a robust encryption scheme, using NTRUEncrypt and ChaCha20-Poly1305 algorithms."

What is Ransomware? | Enterprise Networking Planet

Source: https://www.enterprisenetworkingplanet.com/security/what-is-ransomware/

From the Article: "Ransomware is a type of malicious software that utilizes encryption to take control of a user's or organization's crucial data and demand a ransom — typically in the form of Bitcoin or other digital currency."

What Can Schools Do Against the Onslaught of Ransomware? - Government Technology

Source: https://www.govtech.com/security/what-can-schools-do-against-the-onslaught-of-ransomware

From the Article: "Cyber attacks have become a pressing issue for K-12 schools, but school districts aren't waging the fight alone."

Link back to Table of Contents

Ransomware, DDoS see major upsurge led by upstart hacker group - TechRepublic

Source: https://www.techrepublic.com/article/ransomware-ddos-major-upsurge-led-upstart-hacker-group/

From the Article: "According to NCC Group's Global Threat Intelligence team, November saw a 41% increase in ransomware attacks from 188 incidents to 265. In its most recent Monthly Threat Pulse (you can subscribe to the downloadable report here), the group reported that the month was the most active for ransomware attacks since April this year."

Vice Society ransomware gang switches to new custom encryptor - Bleeping Computer

Source: https://www.bleepingcomputer.com/news/security/vice-society-ransomware-gang-switches-to-new-custom-encryptor/

From the Article: "According to cybersecurity firm SentinelOne, which discovered the new strain and named it "PolyVice," it's likely that Vice Society sourced it from a vendor who supplies similar tools to other ransomware groups."

Moody's says ransomware attack on electric utility in Colombia highlights sector risks

Source: https://insidecybersecurity.com/daily-news/moody%E2%80%99s-says-ransomware-attack-electric-utility-colombia-highlights-sector-risks

From the Article: "A ransomware attack on business-side operations of an electric utility in South America demonstrates security risks facing the electricity sector globally that, among other outcomes, could lead to "regulatory scrutiny, litigation, and a need to boost investment in securing a company's digital systems," Moody's Investors Service said in a report."

Chinese Electric Automaker Nio Hit by Ransomware Attack - Insurance Journal

Source: https://www.insurancejournal.com/news/international/2022/12/22/700516.htm

From the Article: "China-based Nio Inc. said on Tuesday that hackers had breached its computer systems and accessed data on users and vehicle sales, in the latest hacking

incident to hit the global auto industry."

Malware in search ads, Guardian hit with ransomware, Okta source code - CISO Series

Source: https://cisoseries.com/cyber-security-headlines-malware-in-search-ads-guardian-hit-with-ransomware-okta-source-code-accessed/

From the Article: "A new public service announcement from the law enforcement agency warned of threat actors purchasing ads in search engines that spoof legitimate businesses and services. These link back to malicious sites that prompt downloads with names that indicate the software relates to the spoofed company."

Tesla competitor faces Bitcoin ransomware attack during economic crisis

Source: https://www.crypto-news-flash.com/tesla-competitor-faces-bitcoin-ransomware-attack-during-economic-crisis/

From the Article: "It stated that it was made aware that certain of its user information was sold on the internet by third-parties for illegal purposes on Dec. 20. This included data on its vehicle sales in China before August 2021."

Queensland University of Technology shuts IT systems after being hit by ransomware attack

Source: https://www.abc.net.au/news/2022-12-22/qld-qut-cyber-attack-printers-royal/101802692

From the Article: "QUT Vice-Chancellor Professor Margaret Sheil said her own printer was among those affected this morning."

FBI warns of search engine ads pushing malware, phishing - Bleeping Computer

Source: https://www.bleepingcomputer.com/news/security/fbi-warns-of-search-engine-ads-pushing-malware-phishing/

From the Article: "The FBI warns that threat actors are using search engine advertisements to promote websites distributing ransomware or stealing login

credentials for financial institutions and crypto exchanges."

Play ransomware attacks use a new exploit to bypass ProxyNotShell mitigations on ...

Source: https://securityaffairs.co/wordpress/139897/cyber-crime/play-ransomware-bypass-proxynotshell-mitigation.html

From the Article: "Play ransomware operators target Exchange servers using a new exploit chain, dubbed OWASSRF by Crowdstrike, that bypasses Microsoft's mitigations for ProxyNotShell vulnerabilities."

Beware of Cyber Attacks During the Holiday Season – Royal Ransomware ... - Baker Donelson

Source: https://www.bakerdonelson.com/beware-of-cyber-attacks-during-the-holiday-season-royal-ransomware-group-highlighted-as-threats-to-the-health-and-public-health-sectors

From the Article: "Statistics show that cybercrime increases significantly during the holiday season. Threat actors anticipate that workers are distracted and more likely to fall victim to a phishing email scam than any other time of the year. Many employees are out of the office during the holiday season, including IT staff."

CISA Warns Healthcare Organizations of Cuba Ransomware Threat | HealthTech Magazine

Source: https://healthtechmagazine.net/article/2022/12/cisa-warns-healthcare-organizations-cuba-ransomware-threat

From the Article: "Cuba ransomware actors have gained entry to the systems of healthcare and other critical infrastructure sectors through known software vulnerabilities, phishing campaigns, compromised credentials and remote desktop protocol tools."

The Average Cost of a Ransomware Attack in 2022 - EarthWeb

Source: https://earthweb.com/average-cost-of-a-ransomware-attack/

Link back to Table of Contents

From the Article: "A malware attack that encrypts the victim's information and data is called ransomware since the attackers demand ransom to regain the victim's access to their data and device."

Inside Jobs, Cloud Abuse and Ransomware Attacks Are 2023's Top Cybersecurity Threats

Source: https://fintechnews.sg/67677/security/inside-jobs-cloud-abuse-and-ransomware-attacks-are-2023s-top-cybersecurity-threats/

From the Article: "Persistent insider threats, cloud infrastructure misuse and abuse, and the sophistication of cyberattacks are fostering a riskier cyber environment for organizations worldwide."

Holiday Season Sees Onslaught of Ransomware, DDoS Attacks - TechNewsWorld

Source: https://www.technewsworld.com/story/holiday-season-sees-onslaught-of-ransomware-ddos-attacks-177544.html

From the Article: "Ransomware and distributed denial-of-service attacks significantly increased from October to November of this year, a cybersecurity research company reported Tuesday."

Loot from NZ ransomware attack being sold on dark web | Insurance Business New Zealand

Source: https://www.insurancebusinessmag.com/nz/news/cyber/loot-from-nz-ransomware-attack-being-sold-on-dark-web-431229.aspx

From the Article: "Some of Mercury IT's clients whose data have been found for sale include health insurer Accuro, commercial flooring business Polyflor, business mentoring programme Business Central, and architecture firm Catalyst Group."

Hackers bombard PyPi platform with information-stealing malware - Bleeping Computer

Source: https://www.bleepingcomputer.com/news/security/hackers-bombard-pypi-

platform-with-information-stealing-malware/

From the Article: "The PyPi python package repository is being bombarded by a wave of information-stealing malware hiding inside malicious packages uploaded to the platform to steal software developers' data."

OPINION | AIIMS Ransomware Attack: The Missing Picture - News18

Source: https://www.news18.com/news/opinion/opinion-aiims-ransomware-attack-the-missing-picture-6659503.html

From the Article: "On November 23, AIIMS Delhi reported a cyberattack on its e-hospital server which handled inpatient and outpatient digital hospital services, appointment system, smart lab, billing, and report generation."

New Zealand businesses ransomed by LockBit 3.0 after Mercury IT cyberattack

Source: https://techmonitor.ai/technology/cybersecurity/mercury-it-cyberattack-new-zealand-lockbit-ransomware

From the Article: "A ransomware attack by cybercrime gang LockBit 3.0 on New Zealand-based managed service provider Mercury IT appears to have led to numerous organisations from NZ appearing on the gang's dark web victim blog."

Brooklyn hospital network reverts to paper charts for weeks after cyberattack | CNN Business

Source: https://www.cnn.com/2022/12/20/tech/hospital-ransomware/index.html

From the Article: "A network of three hospitals in Brooklyn, New York, has had to work off paper charts for weeks following a cyberattack on its computer systems in late November, the hospital group's chief executive told CNN Monday."

A Computer Weekly buyer's guide to anti-ransomware | TechTarget

Source: https://www.computerweekly.com/ehandbook/A-Computer-Weekly-buyers-guide-to-anti-ransomware

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

From the Article: "The threat of ransomware looms large over business. In this 16-page buyer's guide, Computer Weekly looks at prevention methods, data defence and how to minimise the impact of a potential attack."

Nokoyawa Ransomware: Rust or Bust - Security Boulevard

Source: https://securityboulevard.com/2022/12/nokoyawa-ransomware-rust-or-bust/

From the Article: "The threat group behind Nokoyawa performs double extortion ransomware attacks: exfiltrating sensitive information from organizations, followed by file encryption and a ransom payment demand."

2022's 4 Most Common Cyberattack Patterns - Security Intelligence

Source: https://securityintelligence.com/articles/most-common-cyberattack-patterns-2022/

From the Article: "Ransomware attacks typically follow roughly the same pattern."

Cyber-proofing the healthcare industry from ransomware attacks

Source: https://www.expresshealthcare.in/news/cyber-proofing-the-healthcare-industry-from-ransomware-attacks/437370/

From the Article: "India, which aims to have a USD 5 trillion economy and a trillion-dollar digital component by 2025, has struggled to establish a secure and safe digital arena. There has been tremendous growth in the number of people who have access to internet resources, with millions of users now having online access. "

Mimecast report highlights ransomware risk and impact on UAE organisations

Source: https://www.tahawultech.com/news/mimecast-report-highlights-ransomware-risk-and-impact-on-uae-organisations/

From the Article: "The report found that 59% of cybersecurity leaders in the UAE have seen the number of cybersecurity attacks increase or stay the same over the past year,

with 39% saying they've experienced significant downtime due to a ransomware attack."

Cybercrime (and Security) Predictions for 2023 - The Hacker News

Source: https://thehackernews.com/2022/12/cybercrime-and-security-predictions-for.html

From the Article: "Threat actors continue to adapt to the latest technologies, practices, and even data privacy laws—and it's up to organizations to stay one step ahead by implementing strong cybersecurity measures and programs."

REC Silicon targeted by ransomware attack - Yahoo News

Source: https://columbiabasinherald.com/news/2022/dec/19/rec-silicon-targeted-ransomware-attack/

From the Article: " According to a press release Monday from REC Silicon ASA, the company's virtual server environment suffered a ransomware attack that caused business systems to stop functioning for a brief period of time."

Behind ransomware attacks, a criminal ecosystem that continues to flourish - Globe Echo

Source: https://globeecho.com/news/europe/france/behind-ransomware-attacks-a-criminal-ecosystem-that-continues-to-flourish/

From the Article: "For Bangkok Airways, the trouble started with a post on a discussion forum. In July 2021, the company specializing in security KELA discovers that an Internet user using the pseudonym "babam" is offering remote access to the Thai airline's computer network for sale."

5 types of malicious codes attack millions of computers in VN - VietNamNet

Source: https://vietnamnet.vn/en/5-types-of-malicious-codes-attack-millions-of-computers-in-vn-2092336.html

From the Article: "Trojan may have penetrated the two-layer security scheme; the

number of computers infected with APT malware is at a high level; ransomware has redirected attacks to hosts; online phishing has boomed; and there are challenges from cryptocurrencies."

Healthcare: Essential Defenses for Combating Ransomware - BankInfoSecurity
Source: https://www.bankinfosecurity.com/healthcare-essential-defenses-for-combating-ransomware-a-20738

From the Article: "To avoid having to even consider paying a ransom, experts have long urged all organizations to put better defenses in place, and the healthcare sector is no exception."

Ransomware attack shuts down operations of firefighters at 85 Australian fire stations

Source: https://www.securitynewspaper.com/2022/12/19/ransomware-attack-shuts-down-operations-of-firefighters-at-85-australian-fire-stations/

From the Article: "Fire Rescue Victoria's (FRV) emails, phones, and emergency dispatch systems that automate firefighters' tasks, such as opening station doors as soon as firefighters get an emergency call, were all affected by a hack, which resulted in "a broad IT outage.""

NCC Group: Ransomware attacks increased 41% in November - TechTarget

Source: https://www.techtarget.com/searchsecurity/news/252528505/NCC-Group-Ransomware-attacks-increased-41-in-November

From the Article: "A common thread of NCC Group's November Threat Pulse was a "month full of surprises," particularly related to unexpected shifts in threat actor behavior. The Cuba ransomware gang resurged with its highest number of attacks recorded by NCC Group and Royal replaced LockBit 3.0 as the most active strain, a first since September of last year."

Palo Alto Ignite Reveals The Biggest Cybersecurity Threats of 2022 | BizTech Magazine

Source: https://biztechmagazine.com/article/2022/12/palo-alto-ignite-reveals-biggest-cybersecurity-threats-2022

Link back to Table of Contents

From the Article: "These days, every organization comes up against cybercriminals. Each new device, user or data point expands the attack surface, giving threat actors more opportunities to compromise environments."

CFOs learn how to respond and lead during a cyberattack - CNBC

Source: https://www.cnbc.com/2022/12/19/cfos-learn-how-to-respond-and-lead-during-a-cyberattack.html

From the Article: "That's worrisome enough, but the next morning your CIO delivers this bombshell: Hackers are demanding $4.5 million in ransomware or all that sensitive customer data winds up on the dark web."

Three Ways Schools Can Fend Off Ransomware Attacks | Alvarez & Marsal

Source: https://www.alvarezandmarsal.com/insights/three-ways-schools-can-fend-ransomware-attacks

From the Article: "IT infrastructure and cyber attacks are not always top of mind when it comes to educational institutions. But the reality is that there have been a string of notable attacks against school systems across the country. "

Microsoft: Achilles macOS bug lets hackers bypass Gatekeeper - Bleeping Computer

Source: https://www.bleepingcomputer.com/news/security/microsoft-achilles-macos-bug-lets-hackers-bypass-gatekeeper/

From the Article: "Apple has fixed a vulnerability attackers could leverage to deploy malware on vulnerable macOS devices via untrusted applications capable of bypassing Gatekeeper application execution restrictions."

Louise W. Eggleston Center, Inc. Reports Data Breach Following Ransomware Attack

Source: https://www.jdsupra.com/legalnews/louise-w-eggleston-center-inc-reports-8793936/

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

From the Article: "According to Eggleston, the breach resulted in consumers' full names, Social Security numbers, driver's license numbers, non-driver ID numbers, financial account numbers and access codes, and military ID numbers being compromised. "

10-day countdown: Ransomware gang posts $1.5m demand for files stolen from provider to ...

Source: https://www.nzherald.co.nz/business/24-hour-countdown-ransomware-gang-posts-15m-demand-for-files-stolen-from-provider-to-health-nz-coroners-court-others/HSZ57TXSUFHOHNB7GMB3PNLLCQ/

From the Article: "A gang called LockBit has posted a series time-pressure demands for money on the dark web, claiming to have files from clients to Wellington-based IT provider Mercury IT - which was hit by a ransomware attack in late November, according to the Privacy Commissioner."

Security teams urged to prepare for next era of ransomware - SecurityBrief Australia

Source: https://securitybrief.com.au/story/security-teams-urged-to-prepare-for-next-era-of-ransomware

From the Article: "Global cybersecurity firm Trend Micro has published a new report warning that the ransomware industry could be on the verge of a revolution that sees actors expand into other areas of cybercrime or partner with hostile governments and organised crime groups."

The real cost of ransomware – This Week in Ransomware for the week ending Sunday ...

Source: https://www.itworldcanada.com/article/the-real-cost-of-ransomware-this-week-in-ransomware-for-the-week-ending-sunday-december-18th-2022/518888

From the Article: "In 2018, analysts at Cybersecurity Ventures predicted ransomware damages would grow from US$325 million in 2015 to US$20 billion by the year 2020. Those numbers may have seen astronomical at the time."

BlackCat ransomware group leaks files stolen from D.C. convention bureau - StateScoop

Link back to Table of Contents

Source: https://statescoop.com/blackcat-alphv-ransomware-events-dc/

From the Article: "Malicious actors affiliated with the ransomware outfit known alternately as BlackCat and ALPHV published a trove of files last week stolen from Events D.C., the sports and convention authority in Washington."

Huge increase in cost of phishing attacks | SME Magazine

Source: https://www.smeweb.com/2022/12/19/huge-increase-in-cost-of-phishing-attacks/

From the Article: "New research has found that phishing and the use of MFA (Multi-Factor Authentication) fatigue attacks, an extremely effective method used in high-profile breaches, are on the rise."

Ransomware Attack Drives Medicare To Issue New IDs For 254000 Beneficiaries

Source: https://khn.org/morning-breakout/ransomware-attack-drives-medicare-to-issue-new-ids-for-254000-beneficiaries/

From the Article: "The Centers for Medicare and Medicaid Services says that as many as 254,000 IDs may have been compromised in an online attack of a subcontractor."

Ukraine's DELTA military system users targeted by info-stealing malware

Source: https://www.bleepingcomputer.com/news/security/ukraines-delta-military-system-users-targeted-by-info-stealing-malware/

From the Article: "A compromised Ukrainian Ministry of Defense email account was found sending phishing emails and instant messages to users of the 'DELTA' situational awareness program to infect systems with information-stealing malware."

Ransomware Groups to Increase Zero-Day Exploit-Based Access Methods in the Future

Source: https://www.infosecurity-magazine.com/news/ransomware-groups-increase-zeroday/

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

From the Article: "Ransomware groups are expected to tweak their tactics, techniques and procedures (TTPs) and shift their business models as organizations strengthen their cybersecurity measures, law enforcement gets better at tracking down threat actors and governments tighten regulations on cryptocurrencies, according to Trend Micro's latest research paper."

RedDelta Targets European Government Organizations and Continues to Iterate Custom PlugX Variant

Source: https://www.recordedfuture.com/reddelta-targets-european-government-organizations-continues-iterate-custom-plugx-variant

From the Article: "Recorded Futures Insikt Group continues to track activity we attribute to the likely Chinese state-sponsored threat activity group RedDelta targeting organizations within Europe and Southeast Asia using a customized variant of the PlugX backdoor."

Top 5 Attack Surface Risks of 2022

Source: https://www.recordedfuture.com/top-5-attack-surface-risks-of-2022

From the Article: "In a bid to contend with this years most prominent cyber threats, security teams everywhere have been forced to duly advance their understanding of what constitutes an attack surface."

2022 Attack Surface Intelligence Product Recap

Source: https://www.recordedfuture.com/2022-attack-surface-intelligence-product-recap

From the Article: "As 2022 draws to a close, we are wrapping up a successful year here at the Recorded Future Attack Surface Intelligence team."

Threat Intelligence Tweaks That'll Take Your Security to the Next Level

Source: https://www.recordedfuture.com/threat-intelligence-tweaks

From the Article: "And as your knowledge grows, you realize how much more you could

be doing to keep your organization safe. So now that you have the fundamentals covered, whats next?"

Restrictive Laws Push Chinese Cybercrime toward Novel Monetization Techniques Report

Source: https://www.recordedfuture.com/restrictive-laws-push-chinese-cybercrime-toward-novel-monetization-techniques

From the Article: "Despite difficult times and tougher laws, Chinese criminals adopt new cybercrime techniques — changes in dark web markets, predatory lending gangs, and more."

Intelligence Insights: December 2022

Source: https://redcanary.com/blog/intelligence-insights-december-2022/

From the Article: "To track pervasiveness over time, we identify the number of unique customer environments in which we observed a given threat and compare it to what we've seen in previous months."

Celebrate Those Making a Difference in Cybersecurity

Source: https://www.sans.org/blog/celebrate-those-making-a-difference-in-cybersecurity?msc=rss

From the Article: "Discover the 2022 SANS Difference Makers Award winners and how they are influencing the cybersecurity industry."

Ransomware and wiper signed with stolen certificates

Source: https://securelist.com/ransomware-and-wiper-signed-with-stolen-certificates/108350/

From the Article: "On July 17, 2022, Albanian news outlets reported a massive cyberattack that affected Albanian government e-services. A few weeks later, it was revealed that the cyberattacks were part of a coordinated effort likely intended to cripple

the country's computer systems."

Get Ready: Cisco's Top Security Trends For 2023 That You Need To Know About

Source: https://blogs.cisco.com/security/get-ready-ciscos-top-security-trends-for-2023-that-you-need-to-know-about

From the Article: "We recently had the chance to discuss the top trends prediction for 2023 issued by Gartner and what these may mean for CISOs."

Secure Email Threat Defense: Providing critical insight into business risk

Source: https://blogs.cisco.com/security/secure-email-threat-defense-providing-critical-insight-into-business-risk

From the Article: "Attackers specifically craft business email compromise (BEC) and phishing emails using a combination of malicious techniques, expertly selected from an ever-evolving bag of tricks. "

Experts warn of attacks exploiting WordPress gift card plugin

Source: https://securityaffairs.co/wordpress/140004/hacking/wordpress-gift-card-plugin-attacks.html

From the Article: "Threat actors are actively exploiting a critical flaw in the YITH WooCommerce Gift Cards Premium WordPress plugin installed by over 50,000 websites."

Security Affairs newsletter Round 399 by Pierluigi Paganini

Source: https://securityaffairs.co/wordpress/139988/breaking-news/security-affairs-newsletter-round-399-by-pierluigi-paganini.html

From the Article: "A new round of the weekly SecurityAffairs newsletter arrived! Every week the best security articles from Security Affairs free for you in your email box."

Link back to Table of Contents

An Iranian group hacked Israeli CCTV cameras, defense was aware but didn't block it

Source: https://securityaffairs.co/wordpress/139934/hacking/iranian-group-hacked-israeli-cctv-cameras.html

From the Article: "An Iranian group of hackers, known as Moses Staff, had seized control of dozens of Israeli CCTV cameras, the hack was known to the authorities that did nothing to stop it, reported The Times of Israel which had access to a preview of the full investigative report."

A new Zerobot variant spreads by exploiting Apache flaws

Source: https://securityaffairs.co/wordpress/139918/malware/zerobot-spreads-apache-flaws.html

From the Article: "Microsoft Threat Intelligence Center (MSTIC) researchers discovered a new variant of the Zerobot botnet (aka ZeroStresser) that was improved with the capabilities to target more Internet of Things (IoT) devices."

North Korea-linked hackers stole $626 million in virtual assets in 2022

Source: https://securityaffairs.co/wordpress/139909/intelligence/north-korea-cryptocurrency-theft.html

From the Article: "South Korea's spy agency, the National Intelligence Service, estimated that North Korea-linked threat actors have stolen an estimated 1.5 trillion won ($1.2 billion) in cryptocurrency and other virtual assets in the past five years."

Shoemaker Ecco leaks over 60GB of sensitive data for 500+ days

Source: https://securityaffairs.co/wordpress/139885/data-breach/shoemaker-ecco-data-leaks.html

From the Article: "Our research team discovered an exposed instance hosting a trove of data for Ecco. The team has identified that Ecco left 50 indices exposed to the public, with over 60GB of data accessible since June 2021."

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

German industrial giant ThyssenKrupp targeted in a new cyberattack

Source: https://securityaffairs.co/wordpress/139870/hacking/thyssenkrupp-targeted-cyberattack.html

From the Article: "German multinational industrial engineering and steel production giant ThyssenKrupp AG announced that the Materials Services division and corporate headquarters were hit by a cyberattack. At this time the company has yet to disclose the type of attack that hit its systems and no cybercriminal group has yet to claim responsibility for the attack."

Malicious PyPI package posed as SentinelOne SDK to serve info-stealing malware

Source: https://securityaffairs.co/wordpress/139831/cyber-crime/malicious-pypi-package-sentinelone-sdk.html

From the Article: "Cybersecurity researchers at ReversingLabs have discovered a new malicious package, named 'SentinelOne,' on the Python Package Index (PyPI) repository that impersonates a legitimate software development kit (SDK) for SentinelOne."

Experts spotted a variant of the Agenda Ransomware written in Rust

Source: https://securityaffairs.co/wordpress/139811/cyber-crime/agenda-ransomware-rust.html

From the Article: "Researchers spotted a new variant of the Agenda ransomware which is written in the cross-platform programming language Rust."

Fire and rescue service in Victoria, Australia, confirms cyber attack

Source: https://securityaffairs.co/wordpress/139764/cyber-crime/fire-service-victoria-australia-australia.html

From the Article: "The fire and rescue service in the state of Victoria, Australia, has shut down its network and turned to operating manually after a cyberattack."

Link back to Table of Contents

Samba addressed multiple high-severity vulnerabilities

Source: https://securityaffairs.co/wordpress/139760/hacking/samba-multiple-flaws.html

From the Article: "Samba released updates to address multiple vulnerabilities that can be exploited to take control of impacted systems."

Social Blade discloses security breach

Source: https://securityaffairs.co/wordpress/139747/data-breach/social-blade-data-breach.html

From the Article: "Social media analytics service Social Blade disclosed a security breach after a database containing allegedly stolen data from the company was offered for sale."

4 Most Common Cyberattack Patterns from 2022

Source: https://securityintelligence.com/articles/most-common-cyberattack-patterns-2022/

From the Article: "As 2022 comes to an end, cybersecurity teams globally are taking the opportunity to reflect on the past 12 months and draw whatever conclusions and insights they can about the threat landscape."

Don't Wait to Embrace CISA's Vulnerability Management Rules

Source: https://securityintelligence.com/articles/cisa-new-vulnerability-management-initiative/

From the Article: "Vulnerability management is the time-consuming process of finding and patching a seemingly unlimited number of potential risks. The National Institute of Standards and Technology (NIST) reports more than 23,000 new vulnerabilities for 2022, where more than 17,000 are classified as critical."

How Reveton Ransomware-as-a-Service Changed Cybersecurity

Link back to Table of Contents

Source: https://securityintelligence.com/articles/how-reveton-raas-changed-cybersecurity/

From the Article: "In 2012, Reveton ransomware emerged. It's considered to be the first Ransomware-as-a-Service (RaaS) operation ever. Since then, RaaS has enabled gangs with basic technical skills to launch attacks indiscriminately."

The Cybersecurity Takeaway from Twitter's Verification Chaos

Source: https://securityintelligence.com/articles/cybersecurity-twitter-verification-chaos/

From the Article: "Twitter has been verifiably bonkers since electric car and rocket mogul Elon Musk took over and reworked the social network's long-standing verification system."

5 Ways to Improve Holiday Retail and Wholesale Cybersecurity

Source: https://securityintelligence.com/articles/5-improvements-retail-wholesale-holiday-cybersecurity/

From the Article: "It's the most wonderful time of the year for retailers and wholesalers since the holidays help boost year-end profits. The National Retail Federation (NRF) predicts 2022 holiday sales will come in 6% to 8% higher than in 2021."

Okta Source Code Stolen by Hackers

Source: https://www.securityweek.com/okta-source-code-stolen-hackers

From the Article: "Identity and access management solutions provider Okta this week informed customers that some of the company's source code was stolen recently from its GitHub repositories."

Cyber Insurance Analytics Firm CyberCube Raises $50 Million

Source: https://www.securityweek.com/cyber-insurance-analytics-firm-cybercube-raises-50-million

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

From the Article: "CyberCube, a provider of cyber risk analytics for insurance companies, this week announced that it has raised $50 million in a new funding round that brings the total raised by the firm to $105 million."

Zerobot IoT Botnet Adds More Exploits, DDoS Capabilities

Source: https://www.securityweek.com/zerobot-iot-botnet-adds-more-exploits-ddos-capabilities

From the Article: "The recently detailed Internet of Things (IoT) botnet Zerobot has been updated with an expanded list of exploits and distributed denial-of-service (DDoS) capabilities."

Five Ways TikTok Is Seen as Threat to US National Security

Source: https://www.securityweek.com/five-ways-tiktok-seen-threat-us-national-security

From the Article: "Many in the United States see TikTok, the highly popular video-sharing app owned by Beijing-based ByteDance, as a threat to national security."

France Seeks to Protect Hospitals After Series of Cyberattacks

Source: https://www.securityweek.com/france-seeks-protect-hospitals-after-series-cyberattacks

From the Article: "The French government announced a "vast training programme" on Wednesday to help hospital staff guard against hackers after a series of cyberattacks against medical facilities."

FBI Recommends Ad Blockers as Cybercriminals Impersonate Brands in Search Engine Ads

Source: https://www.securityweek.com/fbi-recommends-ad-blockers-cybercriminals-impersonate-brands-search-engine-ads

From the Article: "The Federal Bureau of Investigation (FBI) this week raised the alarm on cybercriminals impersonating brands in advertisements that appear in search engine

results. The agency has advised consumers to use ad blockers to protect themselves from such threats."

Companies Announced Billions in US Government Cybersecurity Contracts in 2022

Source: https://www.securityweek.com/companies-announced-billions-us-government-cybersecurity-contracts-2022

From the Article: "Companies have announced securing billions of dollars in cybersecurity-related contracts with the United States government in 2022."

Godfather Android Banking Trojan Targeting Over 400 Applications

Source: https://www.securityweek.com/godfather-android-banking-trojan-targeting-over-400-applications

From the Article: "The Godfather Android banking trojan has been observed targeting over 400 banking and crypto applications in 16 countries, threat intelligence firm Group-IB warns."

Critical Vulnerabilities Found in Passwordstate Enterprise Password Manager

Source: https://www.securityweek.com/critical-vulnerabilities-found-passwordstate-enterprise-password-manager

From the Article: "Researchers discovered that the Passwordstate enterprise password manager made by Australian company Click Studios is affected by serious vulnerabilities that could allow an unauthenticated attacker to obtain a user's passwords."

Russian APT Gamaredon Changes Tactics in Attacks Targeting Ukraine

Source: https://www.securityweek.com/russian-apt-gamaredon-changes-tactics-attacks-targeting-ukraine

From the Article: "Russia-linked Gamaredon, a hacking group known for providing services to other advanced persistent threat (APT) actors, is one of the most intrusive,

continuously active APTs targeting Ukraine, Palo Alto Networks' Unit 42 warns."

Ransomware Uses New Exploit to Bypass ProxyNotShell Mitigations

Source: https://www.securityweek.com/ransomware-uses-new-exploit-bypass-proxynotshell-mitigations

From the Article: "Recent Play ransomware attacks targeting Exchange servers were observed using a new exploit chain that bypasses Microsoft's ProxyNotShell mitigations."

Critical Vulnerability in Hikvision Wireless Bridges Allows CCTV Hacking

Source: https://www.securityweek.com/critical-vulnerability-hikvision-wireless-bridges-allows-cctv-hacking

From the Article: "Chinese video surveillance company Hikvision has patched a critical vulnerability in some of its wireless bridge products. The flaw can lead to remote CCTV hacking, according to the researchers who found it."

Industrial Giant Thyssenkrupp Again Targeted by Cybercriminals

Source: https://www.securityweek.com/industrial-giant-thyssenkrupp-again-targeted-cybercriminals

From the Article: "German industrial engineering and steel production giant Thyssenkrupp has again confirmed being targeted by cybercriminals."

Ukraine's Delta Military Intelligence Program Targeted by Hackers

Source: https://www.securityweek.com/ukraines-delta-military-intelligence-program-targeted-hackers

From the Article: "According to CERT-UA, the attackers have used hacked email accounts belonging to Ministry of Defense employees, as well as messaging applications, to send out messages informing recipients about the need to update certificates in the Delta system."

Link back to Table of Contents

New 'RisePro' Infostealer Increasingly Popular Among Cybercriminals

Source: https://www.securityweek.com/new-risepro-infostealer-increasingly-popular-among-cybercriminals

From the Article: "A recently identified information stealer named ‘RisePro’ is being distributed by pay-per-install malware downloader service ‘PrivateLoader’, cyberthreat firm Flashpoint reports."

Cisco Warns of Many Old Vulnerabilities Being Exploited in Attacks

Source: https://www.securityweek.com/cisco-warns-many-old-vulnerabilities-being-exploited-attacks

From the Article: "Many of the bugs, which carry severity ratings of ‘critical’ or ‘high’, have been addressed 4-5 years ago, but organizations that haven’t patched their devices continue to be impacted."

Cybersecurity’s Biggest Mistakes of 2022

Source: https://www.sentinelone.com/blog/cybersecuritys-biggest-mistakes-of-2022/

From the Article: "In just a few years, the world of cybersecurity has changed dramatically. New technologies and threats have emerged, old ones have fallen by the wayside, and the stakes have never been higher."

The Good, the Bad and the Ugly in Cybersecurity – Week 51

Source: https://www.sentinelone.com/blog/the-good-the-bad-and-the-ugly-in-cybersecurity-week-51-5/

From the Article: "The latest dose of justice in the cyber threat landscape: U.S. authorities this week seized 48 internet domains selling “booter” and “stresser” services used by low-level hackers to launch powerful Distributed Denial of Service (DDoS) attacks."

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Patch Tuesday's Impact on Cybersecurity Over the Years

Source: https://www.tenable.com/blog/patch-tuesdays-impact-on-cybersecurity-over-the-years

From the Article: "In 2022, rumors of Patch Tuesday's death circulated widely, but ultimately such talk was greatly exaggerated. Yet, these rumors led to soul searching among many IT, security and DevOps teams."

Tenable Cyber Watch: Policing the Metaverse, Securing AI and ML, Daixin's Threat to Hospitals, and Shifting to Integrated Cyber Platforms

Source: https://www.tenable.com/blog/tenable-cyber-watch-policing-the-metaverse-securing-ai-and-ml-daixins-threat-to-hospitals-and

From the Article: "To help you zap those Monday blahs, here's a caffeinated shot of cyber news you can use: Police chiefs must get hip to the metaverse. CISOs are shifting to integrated cybersecurity platforms. There's new guidance for securing ML and AI systems. Hospitals face a ransomware threat from the Daixin cyber gang."

Cybersecurity Snapshot: Phishing Scams, Salary Trends, Metaverse Risks, Log4J Poll

Source: https://www.tenable.com/blog/cybersecurity-snapshot-phishing-scams-salary-trends-metaverse-risks-log4j-poll

From the Article: "Get the latest on worrisome phishing stats; businesses' embrace of the metaverse, come what may; a (small) improvement in CISO job stability; the compensation cost of security leaders; and more!"

State-sponsored activity (and defenses against it). Breaches, ransomware, and social engineering. SHA-1 retired.

Source: https://thecyberwire.com/newsletters/week-that-was/6/49

From the Article: "Developments in Russia's hybrid war against Ukraine. Recent Iranian cyber activity. NSA warns of Chinese cyber threats. Royal ransomware targets the healthcare sector."

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

MoneyMonger malware. GPS jamming in Russia, cyberespionage against Ukraine. So long, SHA-1.

Source: https://thecyberwire.com/newsletters/daily-briefing/11/240

From the Article: "Predatory loan app discovered embedded in mobile apps. GPS disruptions reported in Russian cities. A new cyberespionage campaign hits Ukraine. NSA warns against dismissing Russian offensive cyber capabilities."

Microsoft Details Gatekeeper Bypass Vulnerability in Apple macOS Systems

Source: https://thehackernews.com/2022/12/microsoft-details-gatekeeper-bypass.html

From the Article: "Microsoft has disclosed details of a now-patched security flaw in Apple macOS that could be exploited by an attacker to get around security protections imposed to prevent the execution of malicious applications."

Hackers Breach Okta's GitHub Repositories, Steal Source Code

Source: https://thehackernews.com/2022/12/hackers-breach-oktas-github.html

From the Article: "Okta, a company that provides identity and access management services, disclosed on Wednesday that some of its source code repositories were accessed in an unauthorized manner earlier this month."

W4SP Stealer Discovered in Multiple PyPI Packages Under Various Names

Source: https://thehackernews.com/2022/12/w4sp-stealer-discovered-in-multiple.html

From the Article: "Threat actors have published yet another round of malicious packages to Python Package Index (PyPI) with the goal of delivering information-stealing malware on compromised developer machines."

Critical Security Flaw Reported in Passwordstate Enterprise Password Manager

Link back to Table of Contents

Source: https://thehackernews.com/2022/12/critical-security-flaw-reported-in.html

From the Article: "Multiple high-severity vulnerabilities have been disclosed in Passwordstate password management solution that could be exploited by an unauthenticated remote adversary to obtain a user's plaintext passwords."

Two New Security Flaws Reported in Ghost CMS Blogging Software

Source: https://thehackernews.com/2022/12/two-new-security-flaws-reported-in.html

From the Article: "Cybersecurity researchers have detailed two security flaws in the JavaScript-based blogging platform known as Ghost, one of which could be abused to elevate privileges via specially crafted HTTP requests."

Zerobot Botnet Emerges as a Growing Threat with New Exploits and Capabilities

Source: https://thehackernews.com/2022/12/zerobot-botnet-emerges-as-growing.html

From the Article: "The Zerobot DDoS botnet has received substantial updates that expand on its ability to target more internet-connected devices and scale its network."

Ransomware Hackers Using New Way to Bypass MS Exchange ProxyNotShell Mitigations

Source: https://thehackernews.com/2022/12/ransomware-hackers-using-new-way-to.html

From the Article: "Threat actors affiliated with a ransomware strain known as Play are leveraging a never-before-seen exploit chain that bypasses blocking rules for ProxyNotShell flaws in Microsoft Exchange Server to achieve remote code execution (RCE) through Outlook Web Access (OWA)."

Ukraine's DELTA Military System Users Under Attack from Info Stealing Malware

Source: https://thehackernews.com/2022/12/ukraines-delta-military-system-users.html

From the Article: "The Computer Emergency Response Team of Ukraine (CERT-UA)

Link back to Table of Contents

this week disclosed that users of the Delta situational awareness program received phishing emails from a compromised email account belonging to the Ministry of Defense."

Beware: Cybercriminals Launch New BrasDex Android Trojan Targeting Brazilian Banking Users

Source: https://thehackernews.com/2022/12/beware-cybercriminals-launch-new.html

From the Article: "The threat actors behind the Windows banking malware known as Casbaneiro has been attributed as behind a novel Android trojan called BrasDex that has been observed targeting Brazilian users as part of an ongoing multi-platform campaign."

Researchers Discover Malicious PyPI Package Posing as SentinelOne SDK to Steal Data

Source: https://thehackernews.com/2022/12/researchers-discover-malicious-pypi.html

From the Article: "Cybersecurity researchers have discovered a new malicious package on the Python Package Index (PyPI) repository that impersonates a software development kit (SDK) for SentinelOne, a major cybersecurity company, as part of a campaign dubbed SentinelSneak."

Trojanized Windows 10 Installer Used in Cyberattacks Against Ukrainian Government Entities

Source: https://thehackernews.com/2022/12/trojanized-windows-10-installer-used-in.html

From the Article: "Government entities in Ukraine have been breached as part of a new campaign that leveraged trojanized versions of Windows 10 installer files to conduct post-exploitation activities."

Facebook Cracks Down on Spyware Vendors from U.S., China, Russia, Israel, and India

Source: https://thehackernews.com/2022/12/facebook-cracks-down-on-spyware-vendors.html

Link back to Table of Contents

From the Article: "Meta Platforms disclosed that it took down no less than 200 covert influence operations since 2017 spanning roughly 70 countries across 42 languages."

Minecraft Servers Under Attack: Microsoft Warns About Cross-Platform DDoS Botnet

Source: https://thehackernews.com/2022/12/minecraft-servers-under-attack.html

From the Article: "Microsoft on Thursday flagged a cross-platform botnet that's primarily designed to launch distributed denial-of-service (DDoS) attacks against private Minecraft servers."

CISA Alert: Veeam Backup and Replication Vulnerabilities Being Exploited in Attacks

Source: https://thehackernews.com/2022/12/cisa-alert-veeam-backup-and-replication.html

From the Article: "The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has added two vulnerabilities impacting Veeam Backup & Replication software to its Known Exploited Vulnerabilities (KEV) Catalog, citing evidence of active exploitation in the wild."

Hackers Actively Exploiting Citrix ADC and Gateway Zero-Day Vulnerability

Source: https://thehackernews.com/2022/12/hackers-actively-exploiting-citrix-adc.html

From the Article: "The U.S. National Security Agency (NSA) on Tuesday said a threat actor tracked as APT5 has been actively exploiting a zero-day flaw in Citrix Application Delivery Controller (ADC) and Gateway to take over affected systems."

New Actively Exploited Zero-Day Vulnerability Discovered in Apple Products

Source: https://thehackernews.com/2022/12/new-actively-exploited-zero-day.html

From the Article: "Apple on Tuesday rolled out security updates to iOS, iPadOS, macOS, tvOS, and Safari web browser to address a new zero-day vulnerability that could result in the execution of malicious code."

Link back to Table of Contents

Google Launches OSV-Scanner Tool to Identify Open Source Vulnerabilities

Source: https://thehackernews.com/2022/12/google-launches-largest-distributed.html

From the Article: "Google on Tuesday announced the open source availability of OSV-Scanner, a scanner that aims to offer easy access to vulnerability information about various projects."

Serious Attacks Could Have Been Staged Through This Amazon ECR Public Gallery Vulnerability

Source: https://thehackernews.com/2022/12/serious-attacks-could-have-been-staged.html

From the Article: "A critical security flaw has been disclosed in Amazon Elastic Container Registry (ECR) Public Gallery that could have been potentially exploited to stage a multitude of attacks, according to cloud security firm Lightspin."

Cybersecurity Experts Uncover Inner Workings of Destructive Azov Ransomware

Source: https://thehackernews.com/2022/12/cybersecurity-experts-uncover-inner.html

From the Article: "Cybersecurity researchers have published the inner workings of a new wiper called Azov Ransomware that's deliberately designed to corrupt data and "inflict impeccable damage" to compromised systems."

KmsdBot Botnet Suspected of Being Used as DDoS-for-Hire Service

Source: https://thehackernews.com/2022/12/kmsdbot-botnet-suspected-of-being-used.html

From the Article: "An ongoing analysis of the KmsdBot botnet has raised the possibility that it's a DDoS-for-hire service offered to other threat actors."

Link back to Table of Contents

Zerobot malware now shooting for Apache systems

Source: https://www.theregister.com/2022/12/22/zerobot_microsoft_iot_botnet/

From the Article: "The Zerobot botnet, first detected earlier this month, is expanding the types of Internet of Things (IoT) devices it can compromise by going after Apache systems."

Citrix patches critical ADC flaw the NSA says is already under attack from China

Source: https://www.theregister.com/2022/12/14/chinas_apt5_attacks_citrix_adc_flaw/

From the Article: "The China-linked crime gang APT5 is already attacking a flaw in Citrix's Application Delivery Controller (ADC) and Gateway products that the vendor patched today."

Extra, Extra, VERT Reads All About It: Cybersecurity News for the Week of December 19, 2022

Source: https://www.tripwire.com/state-of-security/vert-cybersecurity-news-december-12-2022

From the Article: "All of us at Tripwire's Vulnerability Exposure and Research Team (VERT) are constantly looking out for interesting stories and developments in the infosec world."

Don't click too quick! FBI warns of malicious search engine ads

Source: https://www.tripwire.com/state-of-security/dont-click-too-quick-fbi-warns-malicious-search-engine-ads

From the Article: "The FBI is warning US consumers that cybercriminals are placing ads in search engine results that impersonate well-known brands, in an attempt to spread ransomware and steal financial information."

Insight into the 2022 Vulnerability Management Report

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Source: https://www.tripwire.com/state-of-security/insight-vulnerability-management-report

From the Article: "This year marks the release of the first 2022 Vulnerability Management Report from Fortra. The report, which was conducted in September 2022, is based on a comprehensive survey of over 390 cybersecurity professionals with the goal of gaining insights into the latest trends, key challenges, and vulnerability management solution preferences."

Simple Steps to Avoid Phishing Attacks During This Festive season

Source: https://www.tripwire.com/state-of-security/simple-steps-avoid-phishing-attacks-during-festive-season

From the Article: "There's usually a surge in online activities during festive periods. People place gift orders and send funds to loved ones, and organizations roll out offers that reflect the spirit of the festivity."

National Cyber Security Centre (NCSC) Annual Review 2022: Highlights and Thoughts

Source: https://www.tripwire.com/state-of-security/ncsc-annual-review-highlights-and-thoughts

From the Article: "The National Cyber Security Centre (NCSC) is the UK's technical authority for cybersecurity. Established in 2016, it has worked to improve online safety and security, and has brought clarity and insight to an increasingly complex online world. "

Flashpoint Year In Review: 2022 Cryptocurrency Threat Landscape

Source: https://flashpoint.io/blog/risk-intelligence-year-in-review-cryptocurrency/

From the Article: "Bitcoin remained the most-discussed crypto in the threat actor community and the most-used crypto for accepting illicit payments this year. Flashpoint analysts identified over 50,000 unique Bitcoin addresses circulating in Flashpoint collections in 2022."

Link back to Table of Contents

"RisePro" Stealer and Pay-Per-Install Malware "PrivateLoader"

Source: https://flashpoint.io/blog/risepro-stealer-and-pay-per-install-malware-privateloader/

From the Article: "RisePro's presence on Russian Market, and the appearance of the stealer as a payload for a pay-per-install service, may indicate its growing popularity—and viability—within the threat actor community."

It's Time to #StopRansomware With Vulnerability Prioritization and Remediation

Source: https://threatconnect.com/blog/its-time-to-stopransomware-with-vulnerability-prioritization-and-remediation/

From the Article: "One of the main tips & guidance from the Cybersecurity and Infrastructure Security Agency (CISA) is to "Keep Calm and Patch On." CISA emphasizes addressing vulnerabilities twice in this section."

IcedID Botnet Distributors Abuse Google PPC to Distribute Malware

Source: https://www.trendmicro.com/en_us/research/22/l/icedid-botnet-distributors-abuse-google-ppc-to-distribute-malware.html

From the Article: "We analyze the latest changes in IcedID botnet from a campaign that abuses Google pay per click (PPC) ads to distribute IcedID via malvertising attacks."

Web3 IPFS Currently Used For Phishing

Source: https://www.trendmicro.com/en_us/research/22/l/web3-ipfs-only-used-for-phishing---so-far.html

From the Article: "We discuss the use of the InterPlanetary File System (IPFS) in phishing attacks."

Diving into an Old Exploit Chain and Discovering 3 new SIP-Bypass Vulnerabilities

Source: https://www.trendmicro.com/en_us/research/22/l/diving-into-an-old-exploit-

chain-and-discovering-3-new-sip-bypas.html

From the Article: "More than two years ago, a researcher, A2nkF demonstrated the exploit chain from root privilege escalation to SIP-Bypass up to arbitrary kernel extension loading. In this blog entry, we will discuss how we discovered 3 more vulnerabilities from the old exploit chain."

Agenda Ransomware Uses Rust to Target More Vital Industries

Source: https://www.trendmicro.com/en_us/research/22/l/agenda-ransomware-uses-rust-to-target-more-vital-industries.html

From the Article: "This year, various ransomware-as-a-service groups have developed versions of their ransomware in Rust, including Agenda. Agenda's Rust variant has targeted vital industries like its Go counterpart. In this blog, we will discuss how the Rust variant works."

Managing Cyber Risk in 2023: The People Element

Source: https://www.trendmicro.com/en_us/ciso/22/e/managing-cyber-risk.html

From the Article: "Explore the latest findings from Trend Micro's Cyber Risk Index (1H'2022) and discover how to enhance cybersecurity risk management across the digital attack surface."

Probing Weaponized Chat Applications Abused in Supply-Chain Attacks

Source: https://www.trendmicro.com/en_us/research/22/l/probing-weaponized-chat-applications-abused-in-supply-chain-atta.html

From the Article: "This report examines the infection chain and the pieces of malware used by malicious actors in supply-chain attacks that leveraged trojanized installers of chat-based customer engagement platforms."

Threat Brief: OWASSRF Vulnerability Exploitation

Source: https://unit42.paloaltonetworks.com/threat-brief-owassrf/

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

From the Article: "We analyze the new exploit method for Microsoft Exchange Server, OWASSRF, noting that all exploit attempts we've observed use the same PowerShell backdoor, which we track as SilverArrow."

Meddler-in-the-Middle Phishing Attacks Explained

Source: https://unit42.paloaltonetworks.com/meddler-phishing-attacks/

From the Article: "Meddler-in-the-Middle (MitM) phishing attacks show how threat actors find ways to get around traditional defenses and advice."

Russia's Trident Ursa (aka Gamaredon APT) Cyber Conflict Operations Unwavering Since Invasion of Ukraine

Source: https://unit42.paloaltonetworks.com/trident-ursa/

From the Article: "Ukraine and its cyber domain has faced ever-increasing threats from Russia. We give a timely update on APT group Trident Ursa (aka Gamaredon)."

Cybersecurity Trends 2023: Securing our hybrid lives

Source: https://www.welivesecurity.com/2022/12/12/cybersecurity-trends-2023-securing-our-hybrid-lives/

From the Article: "ESET experts offer their reflections on what the continued blurring of boundaries between different spheres of life means for our human and social experience – and especially our cybersecurity and privacy."

Cybersecurity for seniors this holiday season: all generations are a target

Source: https://cybersecurity.att.com/blogs/security-essentials/cybersecurity-for-seniors-this-holiday-season-all-generations-are-a-target

From the Article: "During the holiday season, it is essential to take extra precautions when it comes to cybersecurity. Cybercriminals may be more active than usual, looking for ways to exploit unsuspecting users."

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Vulnerability Spotlight: OpenImageIO file processing issues could lead to arbitrary code execution, sensitive information leak and denial of service

Source: https://blog.talosintelligence.com/vulnerability-spotlight-openimageio-file-processing-issues-could-lead-to-arbitrary-code-execution-sensitive-information-leak-and-denial-of-service/

From the Article: "Cisco Talos recently discovered nineteen vulnerabilities in OpenImageIO, an image processing library, which could lead to sensitive information disclosure, denial of service and heap buffer overflows which could further lead to code execution."

How Marvel's Avengers inspire Pinsent Masons CISO to adapt cybersecurity hiring

Source: https://www.csoonline.com/article/3683869/how-marvels-avengers-inspire-pinsent-masons-ciso-to-adapt-cybersecurity-hiring.html

From the Article: "Cybersecurity's ongoing battle with a "skills shortage" has seen the sector lose its way regarding talent hiring and retention, says Christian Toon, CISO at London-based law firm Pinsent Masons. "

IoT Botnet Zerobot Develops Exploits And DDoS Abilities

Source: https://cyberintelmag.com/iot/iot-botnet-zerobot-develops-exploits-and-ddos-abilities/

From the Article: "An upgraded version of the recently described Internet of Things (IoT) botnet Zerobot has a more extended set of exploits and DDoS capabilities."

Insiders worry CISA is too distracted from critical cyber mission

Source: https://www.cyberscoop.com/cisa-dhs-easterly-cyber-mission/

From the Article: "When Congress was still trying to understand the full extent of Russia's 2016 election meddling and growing increasingly anxious about possible cyberattacks on other U.S. targets, lawmakers rallied behind an idea to shore up the

nation’s digital defenses."

Pop-ups From Google are Now Blocked by DuckDuckGo

Source: https://www.cysecurity.news/2022/12/pop-ups-from-google-are-now-blocked-by.html

From the Article: "DuckDuckGo, a search engine, and browser that has been synonymous with privacy and data protection for years, launched a new feature that captures one of the most common pop-up advertisements on the web, Sign in with Google. "

Why Can’t Company Giants Escape Cybersecurity Breaches?

Source: https://www.cysecurity.news/2022/12/why-cant-company-giants-escape.html

From the Article: "Security breaches have constantly been on a rise in recent times. Just last month, in the course of a week, Uber took its internal communications and engineering systems offline after a network compromise but reported Q2 revenue of $2.7 billion. "

FBI: To Install Malware, Hackers are Buying Ad Services

Source: https://www.cysecurity.news/2022/12/fbi-to-install-malware-hackers-are.html

From the Article: "The FBI has recommended the citizens to download an ad blocker in order to safeguard themselves from internet security dangers, as cybercriminals use ads to spread ransomware and steal information."

Cyberattacks on Municipalities Have Reportedly Cost Taxpayers a $379M Since 2020

Source: https://www.cysecurity.news/2022/12/cyberattacks-on-municipalities-have.html

From the Article: "The municipality of WestLake-Gladstone in Manitoba suffered a loss of over $450,000 as a result of a series of cyberattacks in December 2019 after one of its employees opened a malicious link in a phoney email. "

Link back to Table of Contents

Beware of this Android Banking Trojan that Steals Banking Credentials

Source: https://www.cysecurity.news/2022/12/beware-of-this-android-banking-trojan.html

From the Article: "A financial trojan called "Godfather" which is capable of stealing account credentials from more than 400 different banking and cryptocurrency apps is presently targeting Android users in 16 other countries. "

Concerns About Supply Chain Risks Need Strategies

Source: https://www.cysecurity.news/2022/12/concerns-about-supply-chain-risks-need.html

From the Article: "It is common for the security industry to get disturbed when new vulnerabilities are discovered in software. Two new vulnerabilities were reported in OpenSSL in late October and early November 2022, which overwhelmed news feeds."

DDoS Attacks Can Be Mitigated by AI

Source: https://www.cysecurity.news/2022/12/ddos-attacks-can-be-mitigated-by-ai.html

From the Article: "A DDoS protection system is necessary since DDoS attacks are so common. Numerous media and web-based consumer platforms are supported by AI machine learning algorithms currently."

Russian Hackers Targeted an Oil Refinery in a NATO Nation

Source: https://www.cysecurity.news/2022/12/russian-hackers-targeted-oil-refinery.html

From the Article: "A hacker gang with Russian ties attempted to enter a petroleum refining business in a NATO member state in late August, the latest report by Palo Alto's Unit 42 revealed. "

Link back to Table of Contents

Container Verification Bug Allows Malicious Images to Cloud Up Kubernetes

Source: https://www.darkreading.com/cloud/container-verification-bug-malicious-images-free-rein-kubernetes

From the Article: "A complete bypass of the Kyverno security mechanism for container image imports allows cyberattackers to completely take over a Kubernetes pod to steal data and inject malware."

Videoconferencing Worries Grow, With SMBs in Cyberattack Crosshairs

Source: https://www.darkreading.com/application-security/videoconferencing-worries-grow-with-smbs-in-cyberattack-crosshairs

From the Article: "Securing videoconferencing solutions is just one of many IT security challenges small businesses are facing, often with limited financial and human resources."

New Brand of Security Threats Surface in the Cloud

Source: https://www.darkreading.com/cloud/new-brand-of-security-threats-surface-in-the-cloud

From the Article: "Tech Insight report co-produced by Black Hat, Dark Reading, and Omdia examines how cloud security is evolving in a rapid race to beat threat actors to the (cloud) breach."

Zerobot Adds Brute Force, DDoS to Its IoT Attack Arsenal

Source: https://www.darkreading.com/threat-intelligence/zerobot-adds-brute-force-ddos-iot-attack-arsenal

From the Article: "Threat actors continue to evolve the malicious botnet, which has also added a list of new vulnerabilities it can use to target devices."

Eclipse Business Intelligence Reporting Tool 4.11.0 Remote Code Execution

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Source: https://packetstormsecurity.com/files/170326/SA-20221216-0.txt

From the Article: "Eclipse Business Intelligence Reporting Tool versions 4.11.0 and below suffer from a bypass vulnerability that allows for remote code execution."

Ransomware Roundup – Play Ransomware

Source: https://www.fortinet.com/blog/threat-research/ransomware-roundup-play-ransomware

From the Article: "In this week's ransomware roundup, FortiGuard Labs covers the Play ransomware along with protection recommendations. Read our blog to find out more."

Cyber Threats Increasingly Target Video Games

Source: https://www.hackread.com/cyber-threats-video-games/

From the Article: "Video games have become an integral part of our lives, thanks to evolving technology but the gaming industry has also become a lucrative target for cybercriminals. Let’s dig deeper into the constantly increasing number of treats targeting video games and discover how to avoid them."

Vulnerabilities Discovered in Passwordstate Credential Management Solution

Source: https://heimdalsecurity.com/blog/vulnerabilities-discovered-in-passwordstate-credential-management-solution/

From the Article: "Several critical security vulnerabilities have been found in Passwordstate password management solution. The flaws can be leveraged by a cybercriminal to steal a user’s plaintext passwords."

Threat Actors Use Search Engine Ads for Ransomware and Phishing Attacks

Source: https://heimdalsecurity.com/blog/threat-actors-use-ads-for-ransomware-and-phishing-attacks/

From the Article: "Threat actors use search engines to advertise websites that spread

ransomware or steal login credentials. The ads for various impersonated businesses and services appear at the top of search results and guide the victim to websites that spoof almost perfectly the real ones."

Week in review: LastPass breach disaster, online tracking via UID smuggling, ransomware in 2023

Source: https://www.helpnetsecurity.com/2022/12/25/week-in-review-lastpass-breach-disaster-online-tracking-via-uid-smuggling-ransomware-in-2023/

From the Article: "Here's an overview of some of last week's most interesting news, articles, interviews and videos: LastPass says attackers got users' info and password vault data."

Threat predictions for 2023: From hacktivism to cyberwar

Source: https://www.helpnetsecurity.com/2022/12/23/threat-predictions-2023/

From the Article: "When it comes to 2023 threat predictions, Trellix anticipates spikes in geopolitically motivated attacks across Asia and Europe, hacktivism fueled by tensions from opposing political parties, and vulnerabilities in core software supply chains."

Adversarial risk in the age of ransomware

Source: https://www.helpnetsecurity.com/2022/12/22/adversarial-risk-in-the-age-of-ransomware-video/

From the Article: "Éireann Leverett, Technology and Risk Entrepreneur, makes audience think about ransomware risks from more that one perspective, and that includes the perspective of the threat actors."

ENISA reports on Cyber Europe 2022, tests business continuity and crisis management across EU healthcare sector

Source: https://industrialcyber.co/medical/enisa-reports-on-cyber-europe-2022-tests-business-continuity-and-crisis-management-across-eu-healthcare-sector/

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

From the Article: "The European Union Agency for Cybersecurity (ENISA) published on Tuesday an ‘after action’ report of Cyber Europe 2022, the cybersecurity exercise aimed at testing the resilience of the region’s healthcare sector."

Restaurant platform SevenRooms confirms data breach

Source: https://www.malwarebytes.com/blog/news/2022/12/restaurant-platform-sevenrooms-confirms-fallout-from-third-party-vendor-data-breach

From the Article: "SevenRooms, a “guest experience and retention platform” for food establishments and hospitality organisations, has confirmed it has fallen victim to a third party vendor data breach."

Millions of Gemini cryptocurrency exchange user details leaked

Source: https://www.malwarebytes.com/blog/news/2022/12/millions-of-gemini-cryptocurrency-exchange-user-details-leaked

From the Article: "If you’re a user of the Gemini cryptocurrency exchange, it’s time to be on your guard against phishing attacks."

The Risk Of Escalation From Cyberattacks Has Never Been Greater

Source: https://www.wired.com/story/cyberwar-security/

From the Article: "In 2022, an American dressed in his pajamas took down North Korea’s Internet from his living room. Fortunately, there was no reprisal against the United States."

Swatters Used Ring Cameras To Livestream Attacks, Taunt Police

Source: https://arstechnica.com/information-technology/2022/12/swatters-used-ring-cameras-to-livestream-attacks-taunt-police-prosecutors-say/

From the Article: "Federal prosecutors have charged two men with allegedly taking part in a spree of swatting attacks against more than a dozen owners of compromised Ring home security cameras and using that access to livestream the police response on

social media."

Microsoft Discovers WIndows/Linux Botnet Used In DDoS Attacks

Source: https://arstechnica.com/information-technology/2022/12/microsoft-discovers-windows-linux-botnet-used-in-ddos-attacks/

From the Article: "Microsoft researchers have discovered a hybrid Windows-Linux botnet that uses a highly efficient technique to take down Minecraft servers and performs distributed denial-of-service attacks on other platforms."

Iranian state-aligned threat actor targets new victims in cyberespionage and kinetic campaigns

Source: https://www.techrepublic.com/article/iranian-state-threat-actor-targets-new-victims/

From the Article: "TA435 is now employing more aggressive tactics, including the use of real email accounts, malware and confrontational lures to gain access to key accounts. The threat actor targets high-profile and high-security accounts for cyberespionage purposes."

Subscription Required

Germany to send cabinet member to Taiwan for first time in decades

Source: https://asia.nikkei.com/Politics/International-relations/Germany-to-send-cabinet-member-to-Taiwan-for-first-time-in-decades

From the Article: "Education chief expected to tap digital know-how, seek Confucius Institute alternative"

Why China's exports are in the doldrums

Source: https://asia.nikkei.com/Spotlight/Caixin/Why-China-s-exports-are-in-the-doldrums

Link back to Table of Contents

The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

From the Article: "The U.S., EU and ASEAN have all cut back on imports as inflation takes toll"

U.S. sees China as economic bully, seeks united front with allies

Source: https://asia.nikkei.com/Politics/International-relations/US-China-tensions/U.S.-sees-China-as-economic-bully-seeks-united-front-with-allies

From the Article: "Washington wants to forge strategy with Japan and EU against trade retaliation"

Geopolitical rivalries distorting chip market: TSMC CEO

Source: https://asia.nikkei.com/Business/Tech/Semiconductors/Geopolitical-rivalries-distorting-chip-market-TSMC-CEO

From the Article: "Taiwan chipmaker says productivity and efficiency are being 'destroyed'"

TSMC fab in Japan at center of Sony's image sensor kingdom

Source: https://asia.nikkei.com/Business/Tech/Semiconductors/TSMC-fab-in-Japan-at-center-of-Sony-s-image-sensor-kingdom

From the Article: "Supply chain with locally produced chips key to boosting output"

U.S. blacklists China chipmaker YMTC, AI champion Cambricon, others

Source: https://asia.nikkei.com/Economy/Trade-war/U.S.-blacklists-China-chipmaker-YMTC-AI-champion-Cambricon-others

From the Article: "Chip tool maker intended as alternative to ASML also added to Washington's list"

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Sony plans sensor factory in Japan near new TSMC fab

Source: https://asia.nikkei.com/Business/Tech/Semiconductors/Sony-plans-sensor-factory-in-Japan-near-new-TSMC-fab

From the Article: "Exclusive: Multibillion-dollar plant would tap locally produced chips"

U.S. should brace for '10-year' chip curbs against China: analyst

Source: https://asia.nikkei.com/Editor-s-Picks/Interview/U.S.-should-brace-for-10-year-chip-curbs-against-China-analyst

From the Article: "Author of 'Chip War,' Chris Miller says globalization and free trade are not near death"

Inside Samsung's Fold 4 and Japan's hopes for IBM

Source: https://asia.nikkei.com/techAsia/Inside-Samsung-s-Fold-4-and-Japan-s-hopes-for-IBM

From the Article: "The inside story on the Asia tech trends that matter, from Nikkei Asia and the Financial Times"

Japan recruits IBM to regain lost decade in semiconductor tech

Source: https://asia.nikkei.com/Business/Tech/Semiconductors/Japan-recruits-IBM-to-regain-lost-decade-in-semiconductor-tech

From the Article: "U.S. tech giant will help Rapidus mass-produce 2-nm chips"

South Korea's chip ambitions threaten big environmental toll

Source: https://asia.nikkei.com/Spotlight/The-Big-Story/South-Korea-s-chip-ambitions-threaten-big-environmental-toll

From the Article: "As chip giants like Samsung and SK Hynix expand production, locals fear water contamination"

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Europe rejects Chinese chip investments aimed at EV market

Source: https://asia.nikkei.com/Business/Tech/Semiconductors/Europe-rejects-Chinese-chip-investments-aimed-at-EV-market

From the Article: "U.K. and Germany take tougher line amid worries about state influence"

Japan seeks to release rare earths, 10 other critical items from China's grip

Source: https://asia.nikkei.com/Spotlight/Supply-Chain/Japan-seeks-to-release-rare-earths-10-other-critical-items-from-China-s-grip

From the Article: "By stockpiling and finding alternatives, Tokyo hopes to bolster resilience of supply chains"

TSMC in talks to build first Europe chip plant in Germany

Source: https://asia.nikkei.com/Business/Tech/Semiconductors/TSMC-in-talks-to-build-first-Europe-chip-plant-in-Germany

From the Article: "World's biggest chipmaker looks to capitalize on demand from region's car industry"

Supply Chains Upended by Covid Are Back to Normal

Source: https://www.wsj.com/articles/supply-chains-upended-by-covid-are-back-to-normal-11671746729?mod=hp_lead_pos6

From the Article: "The Covid-19 pandemic might not be gone, but the global supply-chain crisis it spawned has abated."

Chinese Semiconductor IPOs Surge as Chip Arms Race Heats Up

Source: https://www.wsj.com/articles/chinese-semiconductor-ipos-surge-as-chip-arms-race-heats-up-11671631201?mod=Searchresults_pos1&page=1

Link back to Table of Contents

The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

From the Article: "Chip makers and related companies raise billions as China tries to advance domestic industry"

Intel's New Compliance Chief Navigates Geopolitics, Supply-Chain Shift

Source: https://www.wsj.com/articles/intels-new-compliance-chief-navigates-geopolitics-supply-chain-shift-11671660303?mod=Searchresults_pos3&page=1

From the Article: "Carol Tate was appointed CCO this year. The chip maker faces a period of political tension and an increasingly challenging economic environment."

WSJ News Exclusive | Supply-Chain Shortfalls Targeted by New Bill

Source: https://www.wsj.com/articles/supply-chain-shortfalls-targeted-by-new-bill-11670905984?mod=Searchresults_pos4&page=1

From the Article: "Sen. Marco Rubio and Rep. Ro Khanna push federal agencies to better coordinate programs to boost manufacturing"

Opinion | How Antitrade Sentiment Helps China

Source: https://www.wsj.com/articles/antitrade-protectionist-help-beijing-china-trade-deficit-gsp-import-export-renew-congress-tariffs-security-11671219035?mod=Searchresults_pos13&page=1

From the Article: "A program that benefits Beijing's competitors expired two years ago, and Congress can't find the will to renew it."

India's Manufacturing Push Takes an Audacious Gamble on Chips

Source: https://www.wsj.com/articles/indias-manufacturing-push-takes-an-audacious-gamble-on-chips-11670946984?mod=Searchresults_pos1&page=1

From the Article: "With generous incentives and help from Taiwan's Foxconn, India is hoping to kick-start a chip fab industry"

Link back to Table of Contents

India's Chip-Making Plans Face a Long Road Ahead

Source: https://www.wsj.com/video/series/tech-news-briefing/indias-chip-making-plans-face-a-long-road-ahead/872C14D2-9D43-4F46-87EB-FEC4EC2AF070?mod=Searchresults_pos2&page=1

From the Article: "India is making an ambitious push into the advanced-semiconductors market as it looks to establish itself as a high-end tech manufacturing alternative to China. But setting up chip plants takes a lot of time and money. WSJ South Asia correspondent Philip Wen joins host Zoe Thomas to discuss."

China's Chip Equipment Imports Plunge in November as U.S. Export Controls Bite

Source: https://www.wsj.com/articles/chinas-chip-equipment-imports-plunge-in-november-as-u-s-export-controls-bite-11671721795?mod=Searchresults_pos18&page=1

From the Article: "Purchases of semiconductor-making machines from overseas fell to lowest level in more than two years"

U.S. Places Top Chinese Memory Chip Maker on Export Blacklist

Source: https://www.wsj.com/articles/u-s-places-top-chinese-memory-chip-maker-on-export-blacklist-11671128773?mod=Searchresults_pos19&page=1

From the Article: "Measure aimed at Yangtze Memory Technologies comes as U.S.-China technology tensions are on the rise"

Rise of Open-Source Intelligence Tests U.S. Spies

Source: https://www.wsj.com/articles/rise-of-open-source-intelligence-tests-u-s-spies-11670710806?mod=hp_lead_pos6

From the Article: "China outpaces efforts by U.S. intelligence agencies to harness power of publicly available data"

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Cyber Insurers Turn Attention to Catastrophic Hacks

Source: https://www.wsj.com/articles/cyber-insurers-turn-attention-to-catastrophic-hacks-11669407185

From the Article: "Carriers are trying to model the financial impact of cyberattacks on systemically important companies"

Opinion | Blockchain Is Much More Than Crypto

Source: https://www.wsj.com/articles/blockchain-is-much-more-than-crypto-david-solomon-goldman-sachs-smart-contracts-11670345993

From the Article: "Regulated financial institutions are well positioned to harness the revolutionary technology."

Sorry, USA, $40 Billion Won't Buy Chip Independence

Source: https://www.bloomberg.com/opinion/articles/2022-12-07/-40-billion-us-semiconductor-plant-won-t-buy-independence

From the Article: "President Biden and Apple's Cook applauded a plan that offers a minuscule share of global chip capacity."

California Probes Cyberattack Against State's Finance Department - Bloomberg

Source: https://www.bloomberg.com/news/articles/2022-12-12/california-finance-department-targeted-in-cybersecurity-attack

From the Article: "California's finance department has been hit by a cybersecurity attack, and a notorious ransomware group is claiming responsibility."

A Ukrainian Steals $25,000 In Bitcoin From Russian Dark Web Drug Market And Gives It To A Kyiv Charity

Source: https://www.forbes.com/sites/thomasbrewster/2022/12/22/russian-dark-web-drug-market-hacked-by-ukrainian-bitcoin-donated-to-kyiv-charity/

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

From the Article: "A Ukrainian says that he broke into the Solaris drug market's master wallet and diverted its funds to a Ukrainian humanitarian charity."

Author Post: Cyber Threat Intelligence, Continuous Compliance And Tech Solutions With John Grim

Source: https://www.forbes.com/sites/forbesbooksauthors/2022/12/13/cyber-threat-intelligence-continuous-compliance-and-tech-solutions-with-john-grim/

From the Article: "I recently spoke with John Grim, the Director of Cyber Threat Intelligence at Experian. John has 25 years of experience in threat intelligence, investigative response, and digital forensics, and is a former US Marine Corps reservist and US Army soldier."

The International Approach To Combat Ransomware Requires Private Sector Cooperation

Source: https://www.forbes.com/sites/forbesbusinesscouncil/2022/12/15/the-international-approach-to-combat-ransomware-requires-private-sector-cooperation/

From the Article: "In late October, 36 countries and the EU gathered for the second annual international Counter Ransomware Initiative (CRI) Summit to continue their mission to combat ransomware on a global scale."

China's Zero-Covid Exit And The Potential For 2023 Supply Chain Disruptions

Source: https://www.forbes.com/sites/willyshih/2022/12/13/chinas-covid-zero-exit-and-the-potential-for-2023-supply-chain-impacts/

From the Article: "One of the reasons Chinese manufacturing is so efficient is the preponderance of "factory cities" – self-contained campuses that include factories, warehouses, office spaces, and housing within a fenced perimeter."

Link back to Table of Contents