Weekly Security Articles 31-March-2023

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.

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.

For a list of events to attend:

Top Cybersecurity Conferences to Attend in 2023

Source: https://securityscorecard.com/blog/top-cybersecurity-conferences-2023

Chip Industry events

Source: https://semiengineering.com/semiconductor-events/

Events - Online

Welcome! You are invited to join a meeting: A Conversation on End-to-End Secure Automotive Software Updates.

Source: https://nyu.zoom.us/meeting/register/tJUkdeugqD8rGtxGjU3-nR1f71NW75eZAVFW

March 31, 2023

Events - In-person

SANS Institute Cybersecurity Training Event - Hands-On Cyber Security Training Taught by Real-World Practitioners

Source: https://www.sans.org/cyber-security-training-events/2023/

April 2-7, 2023

FIC 2023 - Accueil - Forum International de la Cybersécurité

Source: https://europe.forum-fic.com/

April 5-7, 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.

New England Hardware Security Day

Source: https://nehws.org/

April 7, 2023

April 12, 2023| ICIT Spring Briefing: Modernization

Source: https://www.icitbriefing.org/

April 12, 2023

Coming to Chicago: 2023 HIMSS Global Health Conference & Exhibition | HIMSS

Source: https://www.himss.org/news/coming-chicago-2023-himss-global-health-conference-exhibition

April 17-21, 2023

RSAConference

Source: https://www.rsaconference.com/en

April 24-27, 2023

CISO Leaders Summit Australia 2022

Source: https://focusnetwork.co/cisoleaders.com.au/sydney/

May 2, 2023

ThotCon - Chicago's Hacking Conference

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.thotcon.org/

May 19 & 20, 2023

HackMiami X: May 19 – 20, 2023 - HackMiami Conference 2023

Source: https://hackmiami.com/

May 19-20, 2023

IEEE Symposium on Security and Privacy 2023

Source: https://www.ieee-security.org/TC/SP2023/

May 22-25, 2023

MEMS & Sensors Technical Congress Registration

Source: https://discover.semi.org/mems-sensors-technical-congress-2023-registration.html

May 23-24, 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

GS1 Connect

Source: https://www.gs1us.org/education-and-events/events/gs1-connect

June 5-7, 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.

Techno Security & Digital Forensics Conference

Source: https://www.technosecurity.us/

June 5-8, 2023

MIT Partnership for Systems Approaches to Safety and Security (PSASS)

Source: http://psas.scripts.mit.edu/home/2023-stamp-workshop-information/

June 5-9, 2023

Vendor & Third Party Risk Europe - Center for Financial Professionals

Source: https://www.cefpro.com/forthcoming-events/vendor-third-party-risk-europe/

June 12-13, 2023

Infosecurity Europe 2023

Source: https://www.infosecurityeurope.com/en-gb.html

June 20-22, 2023

.conf22 User Conference | Splunk

Source: https://conf.splunk.com/

July 17-20, 2023

Black Hat

Source: https://www.blackhat.com/upcoming.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.

August 5-10, 2023

CIO Leaders Summit Philippines

Source: https://focusnetwork.co/cioleadersphilippines.com/

August 8, 2023

DEF CON 31

Source: https://defcon.org/

August 10-13, 2023

2023 PCI North America Community Meeting

Source: https://events.pcisecuritystandards.org/

September 12-14, 2023

Mind The Sec

Source: https://www.mindthesec.com.br/

September 12-14, 2023

Critical Infrastructure Protection & Resilience Europe

Source: https://www.cipre-expo.com/

September 26-28, 2023

Gartner Security & Risk Management Summit 2023, London, U.K.

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.gartner.com/en/conferences/emea/security-risk-management-uk

September 26-28, 2023

Cloud Expo Asia

Source: https://www.cloudexpoasia.com/

October 11-12, 2023

Les Assises

Source: https://en.lesassisesdelacybersecurite.com/

October 11-14, 2023

GITEX

Source: https://www.gitex.com/conferences

October 16-20, 2023

IEEE PAINE Conference

Source: https://paine-conference.org/

October 24-26, 2023

2023 PCI Europe Community Meeting

Source: https://www.pcisecuritystandards.org/events/

October 24-26

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.

CISO Leaders Summit Thailand

Source: https://focusnetwork.co/cisoleadersthailand.com/

November 7, 2023

CS4CA: Cyber Security for Critical Assets Summit | Nov 2023 | Riyadh

Source: https://mena.cs4ca.com/

November 2023

Defense Manufacturing Conference Information

Source: http://www.dmcmeeting.com/

December 11-14, 2023

Request for Comments

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."

NIST SP 800-223 (Draft) - High-Performance Computing (HPC) Security: Architecture, Threat Analysis, and Security Posture

Source: https://csrc.nist.gov/publications/detail/sp/800-223/draft

Comments due: April 7, 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.

NISTIR 8320D (Draft) - Hardware-Enabled Security: Hardware-Based Confidential Computing
Source: https://csrc.nist.gov/publications/detail/nistir/8320d/draft

Comments due: April 10,2023

SP 800-219 Rev. 1 (Draft) - Automated Secure Configuration Guidance from the macOS Security Compliance Project (mSCP)

Source: https://csrc.nist.gov/publications/detail/sp/800-219/rev-1/draft

Comments due: April 27, 2023

White Paper NIST AI 100-2e2023 (Draft) - Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations

Source: https://csrc.nist.gov/publications/detail/white-paper/2023/03/08/adversarial-machine-learning-taxonomy-and-terminology/draft

Comments due: September 30, 2023

EASA Artificial Intelligence concept paper (proposed Issue 2) open for consultation | EASA

Source: https://www.easa.europa.eu/en/newsroom-and-events/news/easa-artificial-intelligence-concept-paper-proposed-issue-2-open

From the Article: "As a next major step in the implementation of its AI Roadmap, the European Union Aviation Safety Agency (EASA) has released the Issue 2 of its Concept Paper on Artificial Intelligence (AI) and Machine Learning (ML), for a consultation period of 10 weeks. Please use the comment-response document (CRD) to provide feedback to ai@easa.europa.eu."

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-

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-center-of-excellence-nccoe-responding-to-and-recovering-from-a-cyberattack

Additional sources:
https://content.govdelivery.com/accounts/USNIST/bulletins/340e719

https://industrialcyber.co/regulation-standards-and-compliance/nccoe-project-on-manufacturing-focuses-on-respond-and-recover-elements-guides-mitigation-of-cyber-incidents/

Roadmap for the NIST Artificial Intelligence Risk Management Framework (AI RMF 1.0)

Source: https://www.nist.gov/itl/ai-risk-management-framework/roadmap-nist-artificial-intelligence-risk-management-framework-ai

From the Article: "This Roadmap identifies key activities for advancing the AI RMF that could be carried out by NIST in collaboration with private and public sector organizations – or by those organizations independently. NIST's involvement will depend in part on resources available.

Comments on this Roadmap are welcomed by NIST at any time and may refer to specific items that are either missing or incomplete, or express commitments to pursue Roadmap items. Comments should be addressed to AIframework@nist.gov."

Crosswalks to the NIST Artificial Intelligence Risk Management Framework (AI RMF 1.0)

Source: https://www.nist.gov/itl/ai-risk-management-framework/crosswalks-nist-artificial-intelligence-risk-management-framework

From the Article: "The first two crosswalks which have been developed are: Crosswalk AI RMF (1.0) and ISO/IEC FDIS23894 Information technology - Artificial intelligence - Guidance on risk management (January 26, 2023) An illustration of how NIST AI RMF trustworthiness characteristics relate to the OECD Recommendation on AI, Proposed EU AI Act, Executive Order 13960, and Blueprint for an AI Bill of Rights (January 26, 2023)"

Crosswalk AI RMF 1 0 ISO IEC 23894 pdf

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.nist.gov/system/files/documents/2023/01/26/crosswalk_AI_RMF_1_0_ISO_IEC_23894.pdf

Crosswalk AI RMF 1 0 OECD EO AIA BoR pdf

Source:
https://www.nist.gov/system/files/documents/2023/01/26/crosswalk_AI_RMF_1_0_OECD_EO_AIA_BoR.pdf

Patches/Advisories

Siemens RADIUS Client of SIPROTEC 5 Devices
https://www.cisa.gov/news-events/ics-advisories/icsa-23-080-04

Siemens SCALANCE Third-Party
https://www.cisa.gov/news-events/ics-advisories/icsa-23-080-07

VISAM VBASE Automation Base
https://www.cisa.gov/news-events/ics-advisories/icsa-23-080-05

Delta Electronics InfraSuite Device Master
https://www.cisa.gov/news-events/ics-advisories/icsa-23-080-02

Siemens RUGGEDCOM APE1808 Product Family
https://www.cisa.gov/news-events/ics-advisories/icsa-23-080-03

Keysight N6845A Geolocation Server
https://www.cisa.gov/news-events/ics-advisories/icsa-23-080-01

Cisco Releases Security Advisories for Multiple Products
https://www.cisa.gov/news-events/alerts/2023/03/23/cisco-releases-security-advisories-multiple-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.

ABB Pulsar Plus Controller
https://www.cisa.gov/news-events/ics-advisories/icsa-23-082-05

CISA Releases Six Industrial Control Systems Advisories
https://www.cisa.gov/news-events/alerts/2023/03/23/cisa-releases-six-industrial-control-systems-advisories

ProPump and Controls Osprey Pump Controller
https://www.cisa.gov/news-events/ics-advisories/icsa-23-082-06

SAUTER EY-modulo 5 Building Automation Stations
https://www.cisa.gov/news-events/ics-advisories/icsa-23-082-03

RoboDK
https://www.cisa.gov/news-events/ics-advisories/icsa-23-082-01

Schneider Electric IGSS
https://www.cisa.gov/news-events/ics-advisories/icsa-23-082-04

CP Plus KVMS Pro
https://www.cisa.gov/news-events/ics-advisories/icsa-23-082-02

Rockwell Automation ThinManager
https://www.cisa.gov/news-events/ics-advisories/icsa-23-080-06

CISA Releases Eight Industrial Control Systems Advisories
https://www.cisa.gov/news-events/alerts/2023/03/21/cisa-releases-eight-industrial-control-systems-advisories

Review – Public ICS Disclosures – Week of 3-18-23
https://chemical-facility-security-news.blogspot.com/2023/03/review-public-ics-disclosures-week-of-3_25.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.

Patches/Advisories Articles of Interest

Guidance for investigating attacks using CVE-2023-23397

Source: https://www.microsoft.com/en-us/security/blog/2023/03/24/guidance-for-investigating-attacks-using-cve-2023-23397/

From the Article: "This guide provides steps organizations can take to assess whether users have been targeted or compromised by threat actors exploiting CVE-2023-23397. A successful exploit of this vulnerability can result in unauthorized access to an organization's environment by triggering a Net-NTLMv2 hash leak."

CVE-2023-1634

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-1634

From the Article: "A vulnerability was found in OTCMS 6.72. It has been classified as critical. Affected is the function UseCurl of the file /admin/info_deal.php of the component URL Parameter Handler."

Advanced actor targets Fortinet FortiOS in attacks on govt entities

Source: https://securityaffairs.com/143458/hacking/attacks-fortinet-fortios.html

From the Article: "The unknown threat actor is exploiting a vulnerability in Fortinet FortiOS software, tracked as CVE-2022-41328, that may allow a privileged attacker to read and write arbitrary files via crafted CLI commands."

Adobe fixed ColdFusion flaw listed as under active exploit

Source: https://securityaffairs.com/143479/security/adobe-cold-fusion-exploited-bug.html

From the Article: "Software giant Adobe released security updates for ColdFusion versions 2021 and 2018 to resolve a critical flaw, tracked as CVE-2023-26360 (CVSS base score 8.6), that was exploited in very limited 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 Patch Tuesday fix Outlook zero-day actively exploited

Source: https://securityaffairs.com/143486/security/microsoft-patch-tuesday-march-2023.html

From the Article: "Microsoft Patch Tuesday updates for March 2023 addressed 74 vulnerabilities, including a Windows zero-day exploited in ransomware attacks."

Microsoft Warns of Stealthy Outlook Vulnerability Exploited by Russian Hackers

Source: https://thehackernews.com/2023/03/microsoft-warns-of-stealthy-outlook.html

From the Article: "Microsoft on Friday shared guidance to help customers discover indicators of compromise (IoCs) associated with a recently patched Outlook vulnerability. Tracked as CVE-2023-23397 (CVSS score: 9.8), the critical flaw relates to a case of privilege escalation that could be exploited to steal NT Lan Manager (NTLM) hashes and stage a relay attack without requiring any user interaction."

CISA Warns on Unpatched ICS Vulnerabilities Lurking in Critical Infrastructure

Source: https://www.darkreading.com/vulnerabilities-threats/cisa-warns-unpatched-vulnerabilities-ics-critical-infrastructure

From the Article: "The advisory comes the same week as a warning from the EU's ENISA about potential for ransomware attacks on OT systems in the transportation sector."

WooCommerce Payments Plugin Patches Critical Vulnerability

Source: https://informationsecuritybuzz.com/woocommerce-payments-plugin-patches-critical-vulnerability/

From the Article: "Developers of the popular WooCommerce payments plugin recently identified a critical security flaw that could have affected over 500,000 WordPress sites. The plugin, developed by Automattic, offers a fully integrated payment solution for WooCommerce, making it a highly attractive target for cybercriminals seeking to exploit its vulnerabilities."

Link back to Table of Contents

Microsoft shares guidance for investigating attacks exploiting CVE-2023-23397

Source: https://securityaffairs.com/144040/apt/detecting-cve-2023-23397-attacks.html

From the Article: "Microsoft published guidance for investigating attacks exploiting recently patched Outlook vulnerability tracked as CVE-2023-23397."

CISA Alerts on Critical Security Vulnerabilities in Industrial Control Systems

Source: https://thehackernews.com/2023/03/cisa-alerts-on-critical-security.html

From the Article: "The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has released eight Industrial Control Systems (ICS) advisories on Tuesday, warning of critical flaws affecting equipment from Delta Electronics and Rockwell Automation."

CVE-2020-24857

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-24857

From the Article: "Cross Site Scripting vulnerabilty found in IXPManager v.5.6.0 allows attackers to excute arbitrary code via the looking glass component."

CVE-2023-24295

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-24295

From the Article: "A stack overfow in SoftMaker Software GmbH FlexiPDF v3.0.3.0 allows attackers to execute arbitrary code after opening a crafted PDF file."

CVE-2022-3146

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-3146

From the Article: "A flaw was found in tripleo-ansible. Due to an insecure default configuration, the permissions of a sensitive file are not sufficiently restricted. This flaw allows a local attacker to use brute force to explore the relevant directory and discover the file. This issue leads to information disclosure of important configuration details from

the OpenStack deployment."

CVE-2023-0056

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-0056

From the Article: "An uncontrolled resource consumption vulnerability was discovered in HAProxy which could crash the service. This issue could allow an authenticated remote attacker to run a specially crafted malicious server in an OpenShift cluster. The biggest impact is to availability."

CVE-2023-1612

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-1612

From the Article: "A vulnerability, which was classified as critical, was found in Rebuild up to 3.2.3. This affects an unknown part of the file /files/list-file. The manipulation leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used."

CVE-2023-1613

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-1613

From the Article: "A vulnerability has been found in Rebuild up to 3.2.3 and classified as problematic. This vulnerability affects unknown code of the file /feeds/post/publish. The manipulation leads to cross site scripting."

Cisco Patches High-Severity Vulnerabilities in IOS Software

Source: https://www.securityweek.com/cisco-patches-high-severity-vulnerabilities-in-ios-software/

From the Article: "Cisco's semiannual security updates for IOS and IOS XE software resolve high-severity DoS, command injection, and privilege escalation vulnerabilities."

Link back to Table of Contents

Patch Tuesday -> Exploit Wednesday: Pwning Windows Ancillary Function Driver for WinSock (afd.sys) in 24 Hours

Source: https://securityintelligence.com/posts/patch-tuesday-exploit-wednesday-pwning-windows-ancillary-function-driver-winsock/

From the Article: "'Patch Tuesday, Exploit Wednesday' is an old hacker adage that refers to the weaponization of vulnerabilities the day after monthly security patches become publicly available. "

RSA NetWitness Endpoint EDR Agent 12.x Incorrect Access Control / Code Execution

Source: https://packetstormsecurity.com/files/171476/RSA_NETWITNESS_EDR_AGENT_INCORRECT_ACCESS_CONTROL_CVE-2022-47529.txt

From the Article: "RSA NetWitness Endpoint EDR Agent version 12.x suffers from incorrect access controls that allow for code execution. It allows local users to stop the Endpoint Windows agent from sending the events to a SIEM or make the agent run user-supplied commands."

Chrome 111 Update Patches High-Severity Vulnerabilities

Source: https://www.securityweek.com/chrome-111-update-patches-high-severity-vulnerabilities/

From the Article: "The latest Chrome update brings patches for eight vulnerabilities, including seven reported by external researchers."

Windows 11 Snipping Tool Vulnerability Exposes Sensitive Data

Source: https://informationsecuritybuzz.com/windows-11-snipping-tool-exposes-data/

From the Article: "The Windows Snipping Tool has also been discovered to be vulnerable to a serious privacy problem known as "acropalypse," which enables users to partially recover content that has been cut out of an image."

Link back to Table of Contents

Unpatched Samsung Chipset Vulnerabilities Open Android Users to RCE Attacks

Source: https://www.darkreading.com/attacks-breaches/samsung-chipset-vulnerabilities-android-users-rce-attacks

From the Article: "Users of affected devices that want to mitigate risk from the security issues in the Exynos chipsets can turn off Wi-Fi and Voice-over-LTE settings, researchers from Google's Project Zero say."

Cisco Talos reveals WellinTech ICS platform vulnerable to information disclosure, buffer overflow loopholes

Source: https://industrialcyber.co/vulnerabilities/cisco-talos-reveals-wellintech-ics-platform-vulnerable-to-information-disclosure-buffer-overflow-loopholes/

From the Article: "Two vulnerabilities have been identified by Cisco Talos researchers in WellinTech's KingHistorian industrial control systems (ICS) data manager. Talos tested and confirmed that these versions of WellinTech KingHistorian could be exploited by the vulnerabilities."

Zyxel Unauthenticated LAN Remote Code Execution

Source: https://packetstormsecurity.com/files/171422/zyxel_multiple_devices_zhttp_lan_rce.rb.txt

From the Article: "This Metasploit module exploits a buffer overflow in the zhttpd binary (/bin/zhttpd). It is present on more than 40 Zyxel routers and CPE devices. The code execution vulnerability can only be exploited by an attacker if the zhttp webserver is reachable. "

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_2023-033

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. "

Multiple Vulnerabilities in Mozilla Firefox Could Allow for Arbitrary Code Execution

Source: https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-mozilla-firefox-could-allow-for-arbitrary-code-execution_2023-029

From the Article: "Multiple vulnerabilities have been discovered in Mozilla Firefox and Firefox Extended Support Release (ESR), the most severe of which could allow for arbitrary code execution."

Vulnerability Spotlight: Netgear Orbi router vulnerable to arbitrary command execution

Source: https://blog.talosintelligence.com/vulnerability-spotlight-netgear-orbi-router-vulnerable-to-arbitrary-command-execution/

From the Article: "Cisco Talos recently discovered four vulnerabilities in the Netgear Orbi mesh wireless system, including the main hub router and satellite routers that extend the network's range."

Vulnerability Spotlight: WellinTech ICS platform vulnerable to information disclosure, buffer overflow vulnerabilities

Source: https://blog.talosintelligence.com/vulnerability-spotlight-wellintech-ics-platform-vulnerable-to-information-disclosure-buffer-overflow-vulnerabilities/

From the Article: "KingHistorian is a time-series database that allows users to ingest and process large amounts of data from ICS, including built-in statistical analysis."

Podcasts/Videos

TikTok, GitHub, CISA, More CISA, a Little More CISA, Netgear, & DoKwon – SWN #283

Source: https://www.scmagazine.com/podcast-segment/tiktok-github-cisa-more-cisa-a-little-more-cisa-netgear-dokwon-swn-283

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.

AI Hires Humans to Solve Captcha, Amazing Drones, & Buzzword Bingo 2023 Edition – ESW #310

Source: https://www.scmagazine.com/podcast-segment/ai-hires-humans-to-solve-captcha-amazing-drones-buzzword-bingo-2023-edition-esw-310

Bringing Transparency and Security to IoT with ioXt – Grace Burkard – ESW #310

Source: https://www.scmagazine.com/podcast-segment/bringing-transparency-and-security-to-iot-with-ioxt-grace-burkard-esw-310

CFH #13 – Ryan Jamieson

Source: https://www.scmagazine.com/podcast-episode/cfh-13-ryan-jamieson

Simply Cyber: 🔴 March 24's Top Cyber News NOW! - Ep 330 on Apple Podcasts

Source: https://podcasts.apple.com/us/podcast/march-24s-top-cyber-news-now-ep-330/id1590662228?i=1000605781665

Simply Cyber: So Much Cybersecurity Opportunity with Mari Galloway on Apple Podcasts

Source: https://podcasts.apple.com/us/podcast/so-much-cybersecurity-opportunity-with-mari-galloway/id1590662228?i=1000605624597

Simply Cyber: Cyber Attack Path Management Like a Boss on Apple Podcasts

Source: https://podcasts.apple.com/us/podcast/cyber-attack-path-management-like-a-boss/id1590662228?i=1000605624576

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.

Simply Cyber: 🔴 March 23's Top Cyber News NOW! - Ep 329 on Apple Podcasts

Source: https://podcasts.apple.com/us/podcast/march-23s-top-cyber-news-now-ep-329/id1590662228?i=1000605609328

Simply Cyber: 🔴 March 22's Top Cyber News NOW! - Ep 328 on Apple Podcasts

Source: https://podcasts.apple.com/us/podcast/march-22s-top-cyber-news-now-ep-328/id1590662228?i=1000605430100

Simply Cyber: 🔴 March 21's Top Cyber News NOW! - Ep 327 on Apple Podcasts

Source: https://podcasts.apple.com/us/podcast/march-21s-top-cyber-news-now-ep-327/id1590662228?i=1000605221079

Simply Cyber: 🔴 March 20's Top Cyber News NOW! - Ep 326 on Apple Podcasts

Source: https://podcasts.apple.com/us/podcast/march-20s-top-cyber-news-now-ep-326/id1590662228?i=1000605044496

7MS #565: How to Simulate Ransomware with a Monkey

Source: https://7ms.us/7ms-565-how-to-simulate-ransomware-with-a-monkey/

The Hacker Factory: The Community and Marketing Side of Cybersecurity | A Conversation with Britt Kemp | The Hacker Factory Podcast With Phillip Wylie on Apple Podcasts

Source: https://podcasts.apple.com/us/podcast/the-community-and-marketing-side/id1581926992?i=1000605778208

Flying Trojan Horses | TWiT.TV

Source: https://twit.tv/shows/security-now/episodes/915

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.

NO. 374 — AI Response Shaping, SpaceX Blueprints, GPT-4 Innovation Explosion…

Source: https://danielmiessler.com/podcast/no-374-ai-response-shaping-spacex-blueprints-gpt-4-innovation-explosion/

Ep 236 | 3.23.23 Do you have curtains on your house?

Source: https://thecyberwire.com/podcasts/hacking-humans/236/notes

EPISODE 292-Vital News & Updates

Source: https://inteltechniques.com/blog/2023/03/24/the-privacy-security-osint-show-episode-292/

Episode 314 • Photo cropping bombshell, TikTok debates, and real estate scams

Source: https://www.smashingsecurity.com/

Ep 1787 | 3.24.23 Share on LinkedInShare on FacebookShare on Twitter

Tools, alerts, and advisories from CISA. Reply phishing scams. Cl0p goes everywhere with GoAnywhere. EW in the hybrid war, and shields stay up.

Source: https://thecyberwire.com/podcasts/daily-podcast/1787/notes

Ep 1786 | 3.23.23 Share on LinkedInShare on FacebookShare on Twitter

Pyongyang's intelligence services have been busy in cyberspace. Hacktivists exaggerate the effects of their attacks on OT. Ghostwriter is back. A twice-told tale: ineffective cyberwar campaigns.

Source: https://thecyberwire.com/podcasts/daily-podcast/1786/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.

Ep 1785 | 3.22.23 Share on LinkedInShare on FacebookShare on Twitter

Detecting sandbox emulations. VEC supply chain attacks. Updates from the hybrid war. CISA and NSA offer IAM guidance. Other CISA advisories. Baphomet gets cold feet after all.

Source: https://thecyberwire.com/podcasts/daily-podcast/1785/notes

Ep 1784 | 3.21.23 Share on LinkedInShare on FacebookShare on Twitter

Threat group with novel malware operates in SE Asia. Data theft extortion rises. Key findings of Cisco's Cybersecurity Readiness Index. iPhones no longer welcome in Kremlin. Russian cyber auxiliaries & privateers devote increased attention to healthcare.

Source: https://thecyberwire.com/podcasts/daily-podcast/1784/notes

Ep 1783 | 3.20.23 Share on LinkedInShare on FacebookShare on Twitter

Cl0p ransomware at Hitachi Energy. Alleged TikTok surveillance of journalists. Hacktivist auxiliary hits Indian healthcare records. Cyberattack on Latitude: update. BreachForums arrest.

Source: https://thecyberwire.com/podcasts/daily-podcast/1783/notes

Risky Biz News: FTC to scrutinize cloud providers' business practices

Source: https://risky.biz/RBNEWS127/

Risky Biz News: BreachForums shuts down for good

Source: https://risky.biz/RBNEWS126/

Risky Business #700 -- Yevgeny Prigozhin's empire gets owned

Source: https://risky.biz/RB700/

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.

Between Two Nerds: The Balance between Offence and Defence

Source: https://risky.biz/BTN29/

Risky Biz News: Horror show 0days hit Samsung smartphones

Source: https://risky.biz/RBNEWS125/

Why organizations shouldn't fold to cybercriminal requests

Source: https://www.helpnetsecurity.com/2023/03/24/cybercriminal-requests-video/

From the Article: "Organizations worldwide pay ransomware fees instead of implementing solutions to protect themselves. The ransom is just the tip of the iceberg regarding the damage a ransomware attack can wreak."

How to best allocate IT and cybersecurity budgets in 2023

Source: https://www.helpnetsecurity.com/2023/03/20/how-to-allocate-it-cybersecurity-budgets-video/

From the Article: "Despite the economic uncertainty, 57% of organizations plan to increase their cybersecurity budgets in 2023, according to a survey from Arctic Wolf. This highlights a powerful trend: critical needs like security must be addressed even with IT budgets tightening."

Ferrari hit by ransomware attack, customer details compromised - World News - WION

Source: https://www.wionews.com/videos/ferrari-hit-by-ransomware-attack-customer-details-compromised-574292

From the Article: "Ferrari NV said it was hit by a ransomware attack that exposed information on the Italian sports car maker's customers. "Certain data relating to our clients was exposed, including names, addresses, email addresses and telephone numbers," chief executive officer Benedetto Vigna said Monday in a message to clients."

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.

Watch on Demand: Supply Chain & Third-Party Risk Summit Sessions

Source: https://www.securityweek.com/watch-on-demand-supply-chain-third-party-risk-summit-sessions/

From the Article: "Join us for the virtual experience as we bring together security experts to discuss the complex nature of the supply chain problem, best practices for mitigating security issues."

Two viewpoints on the National Cybersecurity Strategy.

Source: https://thecyberwire.com/podcasts/special-edition/51/notes

From the Article: "Earlier this month, the White House released the National Cybersecurity Strategy, the first issued since 2018. The strategy refocuses roles, responsibilities, and resource allocations in the digital ecosystem, with a five pillar approach."

Christian Sorensen, CEO of SightGain, discusses what we saw in terms of cyber attacks throughout the past year.

Source: https://thecyberwire.com/podcasts/interview-selects/152/notes

From the Article: "This interview from March 23rd, 2023 originally aired as a shortened version on the CyberWire Daily Podcast. In this extended interview, Dave Bittner sits down with Christian Sorensen, CEO of SightGain, to discuss what we saw in terms of cyber attacks throughout the past year."

Oakland mayor gives latest on ransomware attack that leaked info of thousands - YouTube

Source: https://www.youtube.com/watch?v=NGM0CFamTAA

From the Article: "At least 4300 current Oakland city employees are at risk of being hacked following a ransomware attack last month."

Detecting sandbox emulations. VEC supply chain attacks. Updates from the hybrid war.

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 and NSA offer IAM guidance. Other CISA advisories. Baphomet gets cold feet after all.

Source: https://thecyberwire.com/podcasts/daily-podcast/1785/notes

From the Article: "Malware could detect sandbox emulations. A VEC supply chain attack. A new APT is active in Russian-occupied sections of Ukraine. An alleged Russian patriot claims responsibility for the D.C. Health Link attack. CISA and NSA offer guidance on identity and access management (IAM)."

Threat group with novel malware operates in SE Asia. Data theft extortion rises. Key findings of Cisco's Cybersecurity Readiness Index. iPhones no longer welcome in Kremlin. Russian cyber auxiliaries & privateers devote increased attention to healthcare.

Source: https://thecyberwire.com/podcasts/daily-podcast/1784/notes

From the Article: "Threat group with novel malware operates in Southeast Asia. Data theft extortion on the rise. Key findings of Cisco's Cybersecurity Readiness Index. iPhones are no longer welcome in the Kremlin. "

Ransomware attack against Hitachi. Are extreme extortion tactics good news? Google Pixel flaw reveals edited image data. Cl0p's approach to its targets.

Source: https://thecyberwire.com/podcasts/privacy-briefing/791/notes

From the Article: "Hitachi Energy says zero-day bug allowed for ransomware attack. Could ransomware attackers' extreme tactics be good news? Google Pixel flaw reveals edited image data. Cl0p's approach to its targets."

Regulations

Defense Federal Acquisition Regulation Supplement: Use of Supplier Performance Risk System (SPRS) Assessments (DFARS Case 2019-D009)

Source: https://public-inspection.federalregister.gov/2023-05671.pdf

Additional sources:
https://insidecybersecurity.com/share/14469

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.

Prohibition on Using a Covered Application Services

Source: https://www.acq.osd.mil/dpap/dars/opencases/farcasenum/far.pdf

From the Article: “Case Number 2023-010. This rule implements OMB Memo M-23-13, “No TikTok on Government Devices” Implementation Guidance, and the No TikTok on Government Devices Act which prohibits software applications owned and operated by ByteDance Limited (covered applications) on Government Devices. Status: DARC Director tasked Acquisition Technology & Information (FAR) Team to draft interim FAR rule. Report due 05/03/2023.”

Prohibition on Certain Semiconductor Products and Services

Source: https://www.acq.osd.mil/dpap/dars/opencases/farcasenum/far.pdf

From the Article: “Case Number 2023-008. Implements section 5949(a) of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2023 to prohibit executive agencies from: 1) procuring or obtaining, or extending or renewing a contract to procure or obtain, any electronic parts, products, or services that include covered semiconductor products or services; or from 2) entering into a contract, or extending or renewing a contract, with an entity to procure or obtain electronic parts or products that include covered semiconductor products or services. Status: DARC Director tasked Acquisition Technology & Information Team to draft proposed FAR rule. Report due 04/05/2023.”

Credit for Lower-Tier Subcontracting

Source: https://www.acq.osd.mil/dpap/dars/opencases/farcasenum/far.pdf

From the Article: “Case Number 2023-009, Part Number 19, 42: Credit for Lower-Tier Subcontracting. Implements section 1614 of the NDAA for FY 2014 (Pub. L. 113-66), as implemented in SBA's final rule published on December 23, 2016 (81 FR 94246), and section 870 of the NDAA for FY 2020 (Pub. L. 116-92) as implemented in SBA's proposed rule published on December 19, 2022 (87 FR 77529), which allows prime contractors to receive credit toward goals in their small business subcontracting plans for subcontracts awarded by their subcontractors. Status: DARC Director tasked Acquisition Small Business (FAR) Team to draft proposed FAR rule. Report due 05/03/2023.”

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.

Prohibition on Certain Procurements from the Xinjiang Uyghur Autonomous Region

Source: https://www.acq.osd.mil/dpap/dars/opencases/dfarscasenum/dfars.pdf

From the Article: "Case Number 2023-D015, Part Number 212, 225, 252: Prohibition on Certain
Procurements from the Xinjiang Uyghur Autonomous Region. Implements section 855 of the NDAA for FY 2023 (Pub. L. 117-263) which repeals section 848 of the NDAA for FY 2022 (Pub. L 117-81) and 10 U.S.C. 4651 note prec. This new interim rule will address the public comments received in response to the 2022-D008 interim rule which was published at 87 FR 76980 on 16 December 2022. Status: DARC Director tasked Acquisition Law International Acquisition team to draft interim DFARS rule. Report due 04/19/2023."

Strategic and Critical Materials Stockpiling Act Reform

Source: https://www.acq.osd.mil/dpap/dars/opencases/dfarscasenum/dfars.pdf

From the Article: "Case Number 2023-D014, Part Number 225: Strategic and Critical Materials Stockpiling Act Reform. Implements section 1411 of the NDAA for FY 2023 (Pub. L. 117-263); which repeals 10 U.S.C. 187 the Strategic Materials Protection Board, and amends 50 U.S.C. 98h-1 section 10, Strategic and Critical Materials Board of Directors. Status: DARC Director tasked Acquisition Law International Acquisition team to draft proposed DFARS rule. Report due 04/12/2023."

Modification of Cooperative Research and Development Project Authority

Source: https://www.acq.osd.mil/dpap/dars/opencases/dfarscasenum/dfars.pdf

From the Article: "Case Number 2023-D013, Part Number 225.8: Modification of Cooperative Research and Development Project Authority. Implements section 211 of the NDAA for FY 2023 (Pub. L. 117-263) which amends 10 U.S.C. 2350a(a) (2) to expand the scope of 225.871, North Atlantic Treaty Organization (NATO) cooperative projects to also include Cooperative Research and Development Projects to include other allied and friendly foreign countries under the European Union and the European Defense Agency, the European Commission, and the Council of the European Union and their suborganizations. Status:DARC Director tasked Acquisition Law International Acquisition team to draft proposed DFARS rule. Report due 04/12/2023."

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.

Prohibition on Procurement of ForeignMade Unmanned Aircraft Systems

Source: https://www.acq.osd.mil/dpap/dars/opencases/dfarscasenum/dfars.pdf

From the Article: "Case Number 2023-D012, Part Number 204, 252: Prohibition on Procurement of ForeignMade Unmanned Aircraft Systems. Implements section 848 of the NDAA for FY 2020 (Pub L. 116-92), as amended by section 817 of the FY 2023 NDAA (Pub. L. 117-263), which prohibits the procurement of certain foreign-made unmanned aircraft systems by the Department of Defense. Status: DARC Director tasked Acquisition Technology & Information Team to draft proposed DFARS rule. Report due date extended to 05/03/2023."

Establishing FAR Part 40

Source: https://www.acq.osd.mil/dpap/dars/opencases/farcasenum/far.pdf

From the Article: "Case Number 2022-010, Part Number 40: Establishing FAR Part 40. The purpose of this case is to amend the FAR to create a new FAR part, part 40, which will be the new location for cybersecurity supply chain requirements in the FAR. Status: DARC Director tasked staff to draft final FAR rule. Report due date extended to 03/29/2023"

Standardizing Cybersecurity Requirements for Unclassified Federal Information Systems

Source: https://www.acq.osd.mil/dpap/dars/opencases/farcasenum/far.pdf

From the Article: "Case Number 2021-019, Part Number 2, 37, 29, 4, 52, 7: Standardizing Cybersecurity Requirements for Unclassified Federal Information Systems. Implements sections 2(i) and 8(b) of Executive Order 14028, Improving the Nation's Cybersecurity, relating to standardizing common cybersecurity contractual requirements across Federal agencies for unclassified Federal information systems, pursuant to Department of Homeland Security recommendations. Status: OFPP identified draft proposed FAR rule issues. OFPP, FAR and DAR staff resolving issues."

Cyber Threat and Incident Reporting and Information Sharing

Source: https://www.acq.osd.mil/dpap/dars/opencases/farcasenum/far.pdf

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: "Case Number 2021-017, Part Number 12,2,39,4,52: Cyber Threat and Incident Reporting and Information Sharing. Implements sections 2(b)-(c), 2(g)(i), 8(b) of Executive Order 14028, Improving the Nation's Cybersecurity, relating to sharing of information about cyber threats and incident information and reporting cyber incidents. Status: OFPP identified draft proposed FAR rule issues. OFPP, FAR and DAR staff resolving issues."

(EO) Strengthening America's Cybersecurity Workforce

Source: https://www.acq.osd.mil/dpap/dars/opencases/farcasenum/far.pdf

From the Article: "Case Number 2019-014, Part Number 12, 2, 39, 52: (EO) Strengthening America's Cybersecurity Workforce. Implements Executive Order 13870 of May 2, 2019, America's Cybersecurity Workforce, which directs agencies to incorporate the NICE Framework lexicon, taxonomy and reporting requirements into contracts for information technology and cybersecurity services. Status: DAR and FAR staff resolving draft proposed FAR rule open issues."

Controlled Unclassified Information

Source: https://www.acq.osd.mil/dpap/dars/opencases/farcasenum/far.pdf

From the Article: "Case Number 2017-016, Part Number 11, 12, 2.1, 27, 35, 4, 52, 7: Controlled Unclassified Information. Implements 1) the National Archives and Records Administration (NARA) Controlled Unclassified information (CUI) program of E.O. 13556, which provides implementing regulations to address agency policies for designating, safeguarding, disseminating, marking, decontrolling, and disposing of CUI; and 2) OMB Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information (January 3, 2017) which provides guidance on PII breaches occurring in cyberspace or through physical acts. Status: FAR and DARS Staffs resolving open issues identified during OIRA review."

Assessing Contractor Implementation of Cybersecurity Requirements

Source: https://www.acq.osd.mil/dpap/dars/opencases/dfarscasenum/dfars.pdf

From the Article: "Case Number 2019-D041, Part Number 204.73, 204.75, 212.301,

Link back to Table of Contents

217.207, 252.204-7019, 252.204-7020, 252.204-7021: Assessing Contractor Implementation of Cybersecurity Requirements. Implements a DoD certification process, known as the Cybersecurity Maturity Model Certification (CMMC), that measures a company's maturity and institutionalization of cybersecurity practices and processes. Partially implements section 1648 of the FY20 NDAA. (See DFARS case 2022-D017 for the NIST SP 800-171 DoD assessment requirements.) Status: DARC Director tasked Adhoc Team to review public comments, draft final DFARS rule. Report due date extended to 04/05/2023."

(EO) DFARS Buy American Act Requirements

Source: https://www.acq.osd.mil/dpap/dars/opencases/dfarscasenum/dfars.pdf

From the Article: "Case Number 2022-D019, Part Number 213, 225, 252: (EO) DFARS Buy American Act Requirements. Implements the requirements of the Executive Order 14005, Ensuring the Future Is Made in All of America by All of America's Workers, dated 25 January 2021 (effective 25 October 2022) in the DFARS. Status: Case manager forwarded draft proposed rule to DARS Regulatory Control Officer. DARS Regulatory Control Officer reviewing."

NIST SP 800-171 DoD Assessment Requirements

Source: https://www.acq.osd.mil/dpap/dars/opencases/dfarscasenum/dfars.pdf

From the Article: "Case Number 2022-D017, Part Number 204, 252: NIST SP 800-171 DoD Assessment Requirements. Implements DoD assessment requirements, which provide a standard DoD-wide methodology for assessing DoD contractor compliance with all security requirements in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations. Status: DARC Director tasked Ad-hoc team to review public comments, draft final DFARS rule. Report due date extended to 04/12/2023."

Modifications to Printed Circuit Board Acquisition Restrictions

Source: https://www.acq.osd.mil/dpap/dars/opencases/dfarscasenum/dfars.pdf

From the Article: "Case Number 2022-D011, Part Number 225: (S) Modifications to Printed Circuit Board Acquisition Restrictions. Implements section 851 of the FY 2022

Link back to Table of Contents

NDAA (Pub. L. 117-81) which amends 10 U.S.C. 2533d, including the effective date of the statute, and section 841 of the FY 2021 NDAA (Pub. L. 116-283), which prohibits acquiring a covered printed circuit board from a covered country, unless a waiver is obtained. Status: DARC Director tasked Acquisition Law Team-International Acquisition Cmte. to draft proposed DFARS rule. Report due date extended to 04/05/2023."

Supply Chain Software Security

Source: https://www.acq.osd.mil/dpap/dars/opencases/farcasenum/far.pdf

From the Article: "Case Number 2023-002, Part Number 1, 39, 52: Supply Chain Software Security. Implements section 4(n) of Executive Order (EO) 14028, which requires suppliers of software available for purchase by agencies to comply with, and attest to complying with, applicable secure software development requirements in accordance. Status: DARC Director tasked FAR Acquisition Technology & Information Team to draft proposed FAR rule. Report due 04/05/2023."

Enhanced Price Preferences for Critical Components and Critical Items

Source: https://www.acq.osd.mil/dpap/dars/opencases/farcasenum/far.pdf

From the Article: "Case Number 2022-004, Part Number 25: Enhanced Price Preferences for Critical Components and Critical Items. Implements Executive Order 14005, Ensuring the Future Is Made in All of America by All of America's Workers to address the identification of critical products and use of enhanced price preferences. Status: DARC Director tasked Staff to draft proposed FAR rule. Due date extended to 04/05/2023."

Federal Acquisition Supply Chain Security Act of 2018

Source: https://www.acq.osd.mil/dpap/dars/opencases/farcasenum/far.pdf

From the Article: "Case Number 2019-018, Part Number 11, 17, 39, 4, 52, 7, 9: (S) Federal Acquisition Supply Chain Security Act of 2018. Implements the Federal Acquisition Supply Chain Security Act of 2018, which was part of the SECURE Technology Act, Pub. L 115-390(FY19). Status: FAR staff notified DAR staff that CAAC agreed with draft rule as submitted by Team or as modified by DARC."

Link back to Table of Contents

Reports - Government

CONGRESSIONAL BUDGET OFFICE - Spending Reductions That Would Balance the Budget in 2033

Source: https://www.cbo.gov/system/files/2023-03/58984-spendings.pdf

Reports - Industry

Cybersecurity in a digital era | Risk & Resilience

Source: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity-in-a-digital-era

Reshoring Initiative® 2022 Data Report

Source: https://reshorenow.org/content/pdf/2022_Data_Report.pdf

Want US Semiconductor Leadership? Fix the Tax Code

Source: https://www.potomacinstitute.org/featured/2555-want-us-semiconductor-leadership-fix-the-tax-code

White House

FACT SHEET: President Biden Submits to Congress 10-Year Plans to Implement the U.S. Strategy to Prevent Conflict and Promote Stability | The White House

Source: https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/24/fact-sheet-president-biden-submits-to-congress-10-year-plans-to-implement-the-u-s-strategy-to-prevent-conflict-and-promote-stability/

FIVE-ALARM FIRE: The House Freedom Caucus' Extreme Budget Proposal Weakens Our National Security | The White House

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.whitehouse.gov/briefing-room/statements-releases/2023/03/24/five-alarm-fire-the-house-freedom-caucus-extreme-budget-proposal-weakens-our-national-security/

Statement by NSC Spokesperson Adrienne Watson on the Administration's Actions to Invest in Water Security | The White House

Source: https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/22/statement-by-nsc-spokesperson-adrienne-watson-on-the-administrations-actions-to-invest-in-water-security/

FIVE-ALARM FIRE: The House Freedom Caucus' Extreme Budget Proposal Ships Manufacturing Jobs Overseas and Undermines American Workers | The White House

Source: https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/22/five-alarm-fire-the-house-freedom-caucus-extreme-budget-proposal-ships-manufacturing-jobs-overseas-and-undermines-american-workers/

Statement by the President on S. 619, the COVID-19 Origin Act of 2023 | The White House

Source: https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/20/statement-by-the-president-on-s-619-the-covid-19-origin-act-of-2023/

Articles of Interest

COURT DOC: US Federal Agents Arrest Alleged Administrator of Breach Forums "pompompurin"

Source: https://flashpoint.io/blog/usa-vs-conor-brian-fitzpatrick/

From the Article: "On March 17, 2023, US federal agents arrested a New York individual for computer crimes associated with their activities as an administrator of illicit online forum Breach Forums under the online alias "pompompurin.""

Additional sources:
https://thehackernews.com/2023/03/pompompurin-unmasked-infamous.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.

https://www.theregister.com/2023/03/20/in_brief_security/

https://krebsonsecurity.com/2023/03/feds-charge-ny-man-as-breachforums-boss-pompompurin/

https://www.cysecurity.news/2023/03/breachforums-mastermind-pompompurin.html

https://www.engadget.com/us-authorities-arrest-alleged-breachforums-owner-and-fbi-hacker-pompompurin-170009266.html

https://securityaffairs.com/143845/hacking/breachforums-officially-taken-down.html

https://www.techtimes.com/articles/289215/20230319/fbi-arrests-breachforum-owner-hacking-agency-email-servers-2021.htm

https://www.sentinelone.com/blog/the-good-the-bad-and-the-ugly-in-cybersecurity-week-12-4/

https://www.securityweek.com/us-charges-20-year-old-head-of-hacker-site-breachforums/

https://cyberscoop.com/breachforums-arrest-cybercrime-underground/

https://www.theregister.com/2023/03/22/breachforums_shut_down/

https://thehackernews.com/2023/03/breachforums-administrator-baphomet.html

https://www.securityweek.com/new-york-man-arrested-for-running-breachforums-cybercrime-forum/

https://www.securityweek.com/breachforums-shut-down-over-law-enforcement-takeover-concerns/

https://securityaffairs.com/143845/hacking/breachforums-officially-taken-down.html

https://www.reliaquest.com/blog/breachforums-arrest-fbi/

https://www.infosecurity-magazine.com/news/breachforums-admin-arrested-new/

https://www.infosecurity-magazine.com/news/breachforums-shuts-admins-arrest/

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://informationsecuritybuzz.com/fbi-detains-notorious-cybercrime-breachforums/

https://informationsecuritybuzz.com/breachforums-admin-baphomet-closes-hacking-forum/

https://www.malwarebytes.com/blog/news/2023/03/breachforums-to-be-shut-down-after-all-for-fear-of-law-enforcement-infiltration

Ferrari Says Ransomware Attack Exposed Customer Data

Source: https://www.securityweek.com/ferrari-says-ransomware-attack-exposed-customer-data/

From the Article: "Ferrari said that a ransomware attack was responsible for a data breach that exposed customer details, but did not impact company operations."

Additional sources:
https://securityaffairs.com/143784/data-breach/ferrari-confirms-data-breach.html

https://cardealermagazine.co.uk/publish/ferrari-hit-by-ransomware-attack-exposing-customers-details/281493

https://www.insurancejournal.com/news/international/2023/03/21/713146.htm

https://techcrunch.com/2023/03/21/ferrari-says-ransomware-attack-exposed-customers-personal-data/

https://www.bleepingcomputer.com/news/security/ferrari-discloses-data-breach-after-receiving-ransom-demand/

https://www.itsecurityguru.org/2023/03/22/ferrari-data-breach-the-industry-has-its-say/

https://www.infosecurity-magazine.com/news/ferrari-reveals-data-breach-ransom/

https://www.helpnetsecurity.com/2023/03/21/ferrari-data-breach-client-data-exposed/

https://heimdalsecurity.com/blog/ferrari-data-breach-customers-risk-data-leakage/

https://gbhackers.com/ferrari-hacked/

https://www.businesstimes.com.sg/companies-markets/ferrari-says-ransomware-attack-exposed-clients-names-email

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://thewest.com.au/business/automotive/ferrari-reveals-clients-names-addresses-and-emails-exposed-in-ransomware-attack-c-10105184

https://informationsecuritybuzz.com/ferrari-data-breach-ransom-demand/

https://www.hackread.com/ferrari-ransomware-attack-no-ransom/

HinataBot – A New Botnet Could Launch Massive 3.3 Tbps DDoS Attacks

Source: https://gbhackers.com/hinatabot-botnet/

From the Article: "The security analysts at Akamai recently identified a new botnet called HinataBot, based on Golang. Apart from this, HinataBot has been observed exploiting the already-known security flaws in routers and servers to gain unauthorized access to launch DDoS attacks."

Additional sources:
https://cyberintelmag.com/attacks-data-breaches/substantial-3-3-tbps-ddos-attacks-might-be-launched-by-new-hinatabot-botnet/

https://www.blackhatethicalhacking.com/news/akamai-warns-of-new-hinatabot-malware-botnet-capable-of-massive-ddos-attacks/

https://www.cysecurity.news/2023/03/hinatabot-growing-ddos-threat.html

https://www.bleepingcomputer.com/news/security/new-hinatabot-botnet-could-launch-massive-33-tbps-ddos-attacks/

https://www.scmagazine.com/news/malware/go-based-hinatabot-botnet-ddos-attacks

https://heimdalsecurity.com/blog/hinatabot-the-latest-go-based-threat/

https://www.hackread.com/hinatabot-to-launch-ddos-attacks/

https://www.darkreading.com/vulnerabilities-threats/mirai-hackers-golang-bigger-badder-ddos-botnet

Attackers hit Bitcoin ATMs to steal $1.5 million in crypto cash

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.theregister.com/2023/03/23/general_bytes_crypto_atm/

From the Article: "Unidentified miscreants have siphoned cryptocurrency valued at more than $1.5 million from Bitcoin ATMs by exploiting an unknown flaw in digicash delivery systems."

Additional sources:
https://www.hackread.com/cryptoc-atm-general-bytes-bitcoin-theft/

https://securityaffairs.com/143769/cyber-crime/general-bytes-bitcoin-theft.html

https://arstechnica.com/information-technology/2023/03/hackers-drain-bitcoin-atms-of-1-5-million-by-exploiting-0-day-bug/

https://thehackernews.com/2023/03/hackers-steal-over-16-million-in-crypto.html

https://cyberintelmag.com/attacks-data-breaches/1-5m-stolen-from-general-bytes-bitcoin-atms-after-zero-day-exploit/

https://www.blackhatethicalhacking.com/news/general-bytes-bitcoin-atms-hacked-via-zero-day-attack/

https://www.infosecurity-magazine.com/news/general-bytes-bitcoin-atms-hacked/

Malicious ChatGPT Chrome Extension Steal Facebook Accounts

Source: https://gbhackers.com/malicious-chatgpt-chrome-extension/

From the Article: "Thousands of Facebook accounts have been stolen due to a trojanized version of the legitimate ChatGPT extension for Google Chrome."

Additional sources:
https://www.infosecurity-magazine.com/news/malicious-chatgpt-chrome-hijacks/

https://grahamcluley.com/fake-gpt-chrome-extension-steals-facebook-session-cookies-breaks-into-accounts/

https://www.helpnetsecurity.com/2023/03/23/chatgpt-hijacked-facebook/

https://www.darkreading.com/attacks-breaches/malicious-chatgpt-extensions-add-to-google-chrome-woes

Link back to Table of Contents

https://thehackernews.com/2023/03/fake-chatgpt-chrome-browser-extension.html

https://securityaffairs.com/143873/cyber-crime/malicious-chatgpt-extension-for-chrome.html

https://www.hackread.com/fake-chatgpt-extension-hijack-facebook/

ENISA reports ransomware attacks 'most prominent' threat against transport sector, as attacks by hacktivists rise

Source: https://industrialcyber.co/transport/enisa-reports-ransomware-attacks-most-prominent-threat-against-transport-sector-as-attacks-by-hacktivists-rise/

From the Article: "With attacks nearly doubling from 13 percent in 2021 to 25 percent in 2022, ransomware attacks have emerged as the most significant threat to the transportation industry, data released by European Union Agency for Cybersecurity (ENISA) revealed in its initial cyber threat landscape report on the transport sector."

Additional sources:
https://www.tripwire.com/state-of-security/europes-transport-sector-terrorised-ransomware-data-theft-and-denial-service

https://www.securityweek.com/ransomware-will-likely-target-ot-systems-in-eu-transport-sector-enisa/

https://securityaffairs.com/143853/security/enisa-report-transport-sector.html

https://www.helpnetsecurity.com/2023/03/23/transport-sector-cyber-threats/

https://www.bankinfosecurity.com/ransomware-will-target-transport-sector-ot-says-enisa-a-21482

Pwn2Own Vancouver 2023 Day 2: Microsoft Teams, Oracle VirtualBox, and Tesla hacked

Source: https://securityaffairs.com/143950/hacking/pwn2own-vancouver-2023-day-2.html

From the Article: "On the second day of Pwn2Own Vancouver 2023, the organization awarded $475,000 for 10 unique zero-day vulnerabilities."

Link back to Table of Contents

Additional sources:
https://www.darkreading.com/vulnerabilities-threats/tesla-model-3-hacked-2-minutes-pwn2own-contest

https://www.blackhatethicalhacking.com/news/pwn2own-vancouver-2023-zero-day-exploits-revealed-for-tesla-model-3-windows-11-and-macos/

https://securityaffairs.com/143892/hacking/pwn2own-vancouver-2023-day-1.html

https://www.securityweek.com/tesla-hacked-twice-at-pwn2own-exploit-contest/

ShellBot DDoS Malware Targets Linux SSH Servers

Source: https://www.hackread.com/shellbot-malware-targets-linux-ssh-servers/

From the Article: "Poorly managed services refer to weak account credentials, which make the server vulnerable to dictionary attacks. Services such as MS-SQL and RDP (remote desktop protocol) are often targeted."

Additional sources:
https://thehackernews.com/2023/03/new-shellbot-ddos-malware-targeting.html

https://securityaffairs.com/143807/cyber-crime/shellbot-targets-linux-ssh-servers.html

https://heimdalsecurity.com/blog/shellbot-ddos-malware-targets-poorly-managed-linux-servers/

https://gbhackers.com/shell-ddos-malware/

Hitachi Energy Latest Victim of Clop GoAnywhere Attacks - DataBreaches.net

Source: https://www.databreaches.net/hitachi-energy-latest-victim-of-clop-goanywhere-attacks/

From the Article: "Hitachi Energy joined the ranks of victims hit by the Clop ransomware group, which has exploited a zero-day vulnerability in Fortra's widely used managed file transfer software, GoAnywhere MFT. Clop claimed responsibility for the hack, which compromised networks used by 130 different organizations."

Additional sources:

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.techradar.com/news/hitachi-energy-confirms-data-breach-after-being-hit-by-clop-ransomware

https://www.cybersecurityconnect.com.au/commercial/8818-hitachi-energy-hit-by-ransomware-attack-on-third-party-provider

https://heimdalsecurity.com/blog/another-goanywhere-attack-affects-japanese-giant-hitachi-energy/

https://www.securityweek.com/hitachi-energy-blames-data-breach-on-zero-day-as-ransomware-gang-threatens-firm/

NBA Notifying Individuals of Data Breach at Mailing Services Provider

Source: https://www.securityweek.com/nba-notifying-individuals-of-data-breach-at-mailing-services-provider/

From the Article: "NBA is notifying individuals that their information was stolen in a data breach at a third-party mailing services provider."

Additional sources:
https://www.malwarebytes.com/blog/news/2023/03/the-nba-notifies-fans-about-a-data-breach

https://informationsecuritybuzz.com/nba-alerts-hack-third-party-service-provider/

https://gbhackers.com/nba-cyber-incident/

https://www.darkreading.com/risk/cyberattackers-hoop-nba-fan-data-third-party-vendor

UK's NCA infiltrates cybercrime market with fake DDoS sites

Source: https://www.hackread.com/nca-cybercrime-market-fake-ddos-sites/

From the Article: "The National Crime Agency (NCA) has conducted a sting operation to infiltrate the cybercrime market with fake DDoS sites for Operation Power Off."

Additional sources:
https://www.cysecurity.news/2023/03/nca-infiltrates-cybercrime-market-with.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.

https://securityaffairs.com/144011/cyber-crime/nca-fake-ddos-for-hire-sites.html

https://thehackernews.com/2023/03/uk-national-crime-agency-sets-up-fake.html

Dole Says Employee Information Compromised in Ransomware Attack

Source: https://www.securityweek.com/dole-says-employee-information-compromised-in-ransomware-attack/

From the Article: "Dole has admitted in an SEC filing that its investigation into the recent ransomware attack found that the hackers had accessed employee information."

Additional sources:
https://securityaffairs.com/143902/data-breach/dole-food-company-data-breach.html

https://www.infosecurity-magazine.com/news/irish-food-dole-employee-data/

https://www.itsecurityguru.org/2023/03/24/dole-confirms-employee-data-was-breached-following-february-ransomware-attack/

OneNote, Many Problems? The New Phishing Framework

Source: https://securityintelligence.com/onenote-new-phishing-framework/

From the Article: "Their newest hook? OneNote documents. First noticed in December 2022, this phishing framework has seen success in fooling multiple antivirus (AV) tools by using .one file extensions, and January 2023 saw an attack uptick as compromises continued."

Additional sources:
https://thehackernews.com/2023/03/emotet-rises-again-evades-macro.html

https://heimdalsecurity.com/blog/emotet-malware-microsoft-onenote-attachments/

https://www.2-spyware.com/microsoft-onenote-files-used-to-spread-emotet-malware

Critical flaw in WooCommerce Payments plugin allows site takeover

Source: https://securityaffairs.com/143959/security/woocommerce-payments-plugin-

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.

critical-bugs.html

From the Article: "On March 23, 2023, researchers from Wordfence observed that the “WooCommerce Payments – Fully Integrated Solution Built and Supported by Woo” plugin had been updated to version 5.6.2."

Additional sources:
https://www.csoonline.com/article/3691637/critical-flaw-in-woocommerce-can-be-used-to-compromise-wordpress-websites.html

https://www.blackhatethicalhacking.com/news/critical-bug-in-woocommerce-payments-exposes-online-stores-to-hackers/

https://www.securityweek.com/critical-woocommerce-payments-vulnerability-leads-to-site-takeover/

ChatGPT bug leaked users' conversation histories - BBC News

Source: https://www.bbc.com/news/technology-65047304

From the Article: "A ChatGPT glitch allowed some users to see the titles of other users' conversations, the artificial intelligence chatbot's boss has said."

Additional sources:
https://www.hackread.com/chatgpt-bug-conversation-history-titles/

https://thehackernews.com/2023/03/openai-reveals-redis-bug-behind-chatgpt.html

https://www.cysecurity.news/2023/03/users-private-info-accidentally-made.html

MITRE System of Trust focuses on identifying, assessing supply chain security risks; delivers assessment techniques

Source: https://industrialcyber.co/supply-chain-security/mitre-system-of-trust-focuses-on-identifying-assessing-supply-chain-security-risks-delivers-assessment-techniques/

From the Article: "Not-for-profit organization MITRE debuted its System of Trust framework to address supply chain security challenges, providing the foundation needed for understanding supply chain risks."

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.helpnetsecurity.com/2023/03/24/mitre-system-of-trust-risk-model/

https://www.darkreading.com/risk/mitre-rolls-out-supply-chain-security-prototype

Threat actors abuse Adobe Acrobat Sign to distribute RedLine info-stealer

Source: https://securityaffairs.com/143738/hacking/malware-via-adobe-acrobat-sign.html

From the Article: "Avast researchers reported that threat actors are abusing the legitimate Adobe Acrobat Sign service to distribute the RedLine information stealer."

Additional sources:
https://www.cysecurity.news/2023/03/threat-actors-exploit-adobe-acrobat.html

https://www.securityweek.com/adobe-acrobat-sign-abused-to-distribute-malware/

CISA kicks off ransomware vulnerability pilot to help spot ransomware-exploitable flaws

Source: https://www.csoonline.com/article/3691229/cisa-kicks-off-ransomware-vulnerability-pilot-to-help-spot-ransomware-exploitable-flaws.html

From the Article: "Last week, the US Cybersecurity and Infrastructure Security Agency (CISA) announced the launch of the Ransomware Vulnerability Warning Pilot (RVWP) program to "proactively identify information systems that contain security vulnerabilities commonly associated with ransomware attacks." "

Additional sources:
https://industrialcyber.co/cisa/new-jcdc-pre-ransomware-notification-initiative-warns-organizations-could-stop-cyberattacks-before-damage-occurs/

https://www.securitymagazine.com/articles/99086-cisa-starts-ransomware-vulnerability-pilot-program

Android-based banking Trojan Nexus now available as malware-as-a-service

Source: https://www.csoonline.com/article/3691652/android-based-banking-trojan-nexus-now-available-as-malware-as-a-service.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: "Italian cybersecurity firm Cleafy has found “Nexus”, a new Android Trojan capable of hijacking online accounts and siphoning funds from them, to be targeting customers from 450 banks and cryptocurrency services worldwide."

Additional sources:
https://thehackernews.com/2023/03/nexus-new-rising-android-banking-trojan.html

https://www.darkreading.com/mobile/new-android-malware-targets-customers-of-450-financial-institutions-worldwide

Okta Post-Exploitation Method Reveals User Passwords

Source: https://www.cysecurity.news/2023/03/okta-post-exploitation-method-reveals.html

From the Article: "Post-exploitation attack technique has been discovered that enables adversaries to read cleartext user passwords for Okta, the identity access, and management (IAM) provider, acquiring extensive access to the corporate environment. "

Additional sources:
https://www.infosecurity-magazine.com/news/attack-method-affect-okta-passwords/

https://www.darkreading.com/endpoint/okta-post-exploit-method-exposes-user-passwords

Kimsuky's Attacks Alerted German and South Korean Agencies

Source: https://www.cysecurity.news/2023/03/kimsukys-attacks-alerted-german-and.html

From the Article: "In a joint warning issued by the German and South Korean intelligence agencies, it has been noted that a North Korean hacker group named Kimsuky has been increasing cyber-attack tactics against the South Korean network."

Additional sources:
https://thehackernews.com/2023/03/german-and-south-korean-agencies-warn.html

https://informationsecuritybuzz.com/german-south-korean-agencies-alerts-kimsuky-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.

Here's what to expect from lawmakers who will grill TikTok's CEO on privacy, security and child safety

Source: https://cyberscoop.com/tiktok-ceo-congress-lawmakers-hearing-privacy-national-security/

From the Article: "In a highly anticipated congressional hearing, TikTok CEO Shou Chew will testify in front of the House Energy and Commerce Committee Thursday to address lawmakers' concerns about the influence of its Chinese parent company, its approach to dealing with children's mental health issues and overall data security practices."

Additional sources:
https://cyberscoop.com/shou-chew-tiktok-hearing/

CISA Unveils Ransomware Notification Initiative

Source: https://www.infosecurity-magazine.com/news/isa-unveils-ransomware/

From the Article: "Provides businesses with early warnings to evict threat actors before they can encrypt data."
Additional sources:
https://securityaffairs.com/143990/security/cisa-pre-ransomware-notifications-intiative.html

Custom 'Naplistener' Malware a Nightmare for Network-Based Detection

Source: https://www.darkreading.com/threat-intelligence/custom-naplistener-malware-network-based-detection-sleep

From the Article: "Threat actors are using legitimate network assets and open source code to fly under the radar in data-stealing attacks using a set of custom malware bent on evasion."

Additional sources:
https://thehackernews.com/2023/03/new-naplistener-malware-used-by-ref2924.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.

The City of Toronto, Among This Week's Victims of GoAnywhere Attacks

Source: https://heimdalsecurity.com/blog/the-city-of-toronto-among-this-weeks-victims-of-goanywhere-attacks/

From the Article: "The City of Toronto announced a data breach caused by GoAnywhere attacks. Clop ransomware, the gang responsible for exploiting the vulnerability in GoAnywhere also impacted UK's Virgin Red and Pension Protection Fund."

Additional sources:
https://securityaffairs.com/143938/breaking-news/city-of-toronto-clop-ransomware.html

Ex-Meta security staffer accuses Greece of spying on her phone

Source: https://www.theregister.com/2023/03/21/meta_employee_spyware/

From the Article: "Meta's former security policy manager, who split her time between the US and Greece, is reportedly suing the Hellenic national intelligence service for hacking her phone."

Additional sources:
https://gizmodo.com/facebook-meta-security-seaford-predator-spyware-greece-1850243980

IRS Phishing Emails Used to Distribute Emotet

Source: https://www.infosecurity-magazine.com/news/irs-phishing-emails-emotet/

From the Article: "Monster 500MB attachment hides a nasty surprise."

Additional sources:
https://www.malwarebytes.com/blog/news/2023/03/beware-fake-irs-tax-email-delivers-emotet-malware

Streaming Platform Gaint Lionsgate Exposes Over 37m Users' Data

Source: https://gbhackers.com/lionsgate-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.

From the Article: "Lions Gate Entertainment Corporation, doing business as Lionsgate, exposed users' IP addresses and data on the content they saw on its movie-streaming service. According to Cybernews analysts, Lionsgate Play, a video streaming service, had exposed user information via an open ElasticSearch instance."

Additional sources:
https://securityaffairs.com/143886/security/lionsgate-data-leak.html

LockBit Attacks Oakland with Ransomware Twice in as Many Weeks

Source: https://www.cysecurity.news/2023/03/lockbit-attacks-oakland-with-ransomware.html

From the Article: "Following a ransomware attack on LockBit's network last month that caused information from its network to be leaked, the city of Oakland in the state of California has been uploaded to the dark web victim blog. In order to avoid further information from the city being released, the gang has given Oakland's city council until April 10 to begin negotiations."

Additional sources:
https://abc7news.com/oakland-ransomware-city-of-hacking-cyberattack-mayor-sheng-thao/12983940/

CISA unleashes Untitled Goose Tool to honk at danger in Microsoft's cloud

Source: https://www.theregister.com/2023/03/24/cisa_microsoft_cloud_ransomware/

From the Article: "American cybersecurity officials have released an early-warning system to protect Microsoft cloud users."

Additional sources:
https://www.helpnetsecurity.com/2023/03/24/malicious-activity-microsoft-cloud/

3CX VoIP Software Compromise & Supply Chain Threats

Source: https://www.huntress.com/blog/3cx-voip-software-compromise-supply-chain-threats

From the article: "The 3CX VoIP Desktop Application has been compromised to deliver

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.

malware via legitimate 3CX updates. Huntress has been investigating this incident and working to validate and assess the current supply chain threat to the security community."

Nation-State Threat Actors Exploited Zero Days The Most In 2022

Source: https://www.scmagazine.com/news/threat-intelligence/threat-actors-linked-to-nation-states-exploited-zero-days-the-most-in-2022

From the Article: "Threat groups with ties to nation-states were the driving force behind exploiting zero-day vulnerabilities last year, according to a new report by cybersecurity firm Mandiant."

An Arrested Administrator Shut Down the Notorious Hacking Forum

Source: https://www.cysecurity.news/2023/03/an-arrested-administrator-shut-down.html

From the Article: "An FBI officer has arrested a former administrator and owner of an infamous hacker forum that exposed data on companies such as HDB Financial Services, Rail Yatri, Acer, WhatsApp, Truecaller India, Hyundai India, Skoda India, etc. "

FTC extends deadline by six months for compliance with some changes to financial data security rules

Source: https://cybersecurity.att.com/blogs/security-essentials/ftc-extends-deadline-by-six-months-for-compliance-with-some-changes-to-financial-data-security-rules

From the Article: "In a highly connected, internet-powered world, transactions take place online, in person, and even somewhere in between. Given the frequency of digital information exchange on our devices, including smartphones and smart home gadgets, cybersecurity has never been more important for protecting sensitive customer information. "

Italian agency warns ransomware targets known VMware vulnerability

Source: https://cybersecurity.att.com/blogs/security-essentials/italian-agency-warns-ransomware-targets-known-vmware-vulnerability

From the Article: "News broke in early February that the ACN, Italy's National Cybersecurity

Link back to Table of Contents

Agency, issued a warning regarding a VMware vulnerability discovered two years ago. Many organizations hadn't yet patched the issue and became the victims of a new ransomware called ZCryptor."

Anomali Cyber Watch: APT, China, Data leak, Injectors, Packers, Phishing, Ransomware, Russia, and Ukraine

Source: https://www.anomali.com/blog/anomali-cyber-watch-apt-china-data-leak-injectors-packers-phishing-ransomware-russia-and-ukraine

From the Article: "The various threat intelligence stories in this iteration of the Anomali Cyber Watch discuss the following topics: APT, China, Data leak, Injectors, Packers, Phishing, Ransomware, Russia, and Ukraine."

Severe Privacy Vulnerability 'Acropalypse' Affects Windows 11 Snipping Tool

Source: https://www.blackhatethicalhacking.com/news/severe-privacy-vulnerability-acropalypse-affects-windows-11-snipping-tool/

From the Article: "Microsoft's Windows 11 Snipping Tool has been found to contain a severe privacy flaw named 'acropalypse'. The flaw, which has already been discovered in Google Pixel's Markup Tool, allows partially edited content to be recovered. "

Ssh… Don't Tell Them I Am Not HTTPS: How Attackers Use SSH.exe as a Backdoor Into Your Network

Source: https://www.blackhillsinfosec.com/ssh-dont-tell-them-i-am-not-https/

From the Article: "In many cases these binaries are well known, the techniques documented, and (hopefully) the malicious use is detectable by security products or threat hunting processes. However, in a recent incident response engagement, we found a LOLBAS technique that did not fall in that category of well documented. In fact, the technique does not currently appear to be in the MITRE ATT&K framework."

20th March – Threat Intelligence Report

Source: https://research.checkpoint.com/2023/20th-march-threat-intelligence-report/

From the Article: "Check Point IPS, Threat Emulation and Harmony Endpoint provide protection

Link back to Table of Contents

against this threat (GoAnywhere MFT Insecure Deserialization (CVE-2023-0669); Ransomware.Win.Clop)."

Detecting Malicious Packages on PyPI: Malicious package on PyPI use phishing techniques to hide its malicious intent

Source: https://blog.checkpoint.com/2023/03/18/detecting-malicious-packages-on-pypi-malicious-package-on-pypi-use-phishing-techniques-to-hide-its-malicious-intent/

From the Article: "Check Point CloudGuard Spectralops detected a malicious phishing account on PyPI, the leading Python package index. Users installing the account packages were exposed to a malicious actor, probably a PII stealer. Once detected, we alerted PyPI on these packages."

Reality Check on Cybersecurity: 9% of Companies in Europe are Ready to Defend Against Cyber Threats

Source: https://blogs.cisco.com/gov/cybersecurity-europe-companies-not-ready-to-defend-against-cyber-threats

From the Article: "The urgency around addressing the European Union's cyber shortcomings is well founded. A mere 9% of organizations in Europe have the 'Mature' level of readiness needed to be resilient against modern cyber risks, according to Cisco's first-ever Cybersecurity Readiness Index and its Europe Edition."

Regulatory Harmonization in Cyber Incident Reporting: Best Idea for Security?

Source: https://blogs.cisco.com/gov/regulatory-harmonization-in-cyber-incident-reporting

From the Article: " In March 2022, the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) was enacted in the U.S. with a clear purpose to improve the nation's cybersecurity by requiring covered entities to report significant cyber incidents, including payments made for ransomware attacks."

55 zero-day flaws exploited last year show the importance of security risk management

Source: https://www.csoonline.com/article/3691609/55-zero-day-flaws-exploited-last-year-show-the-importance-of-security-risk-management.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: "Deploying security patches as quickly as possible remains one of the best ways to prevent most security breaches, as attackers usually rely on exploits for publicly known vulnerabilities that have a patch available -- the so-called n-day exploits."

Average enterprise storage/backup device has 14 vulnerabilities, three high or critical risks

Source: https://www.csoonline.com/article/3691529/average-enterprise-storage-backup-device-has-14-vulnerabilities-three-high-or-critical-risks.html

From the Article: "The average enterprise storage and backup device has 14 vulnerabilities, three of which are high or critical risk that could present a significant compromise if exploited."

Backslash AppSec solution targets toxic code flows, threat model automation

Source: https://www.csoonline.com/article/3691256/backslash-appsec-solution-targets-toxic-code-flows-threat-model-automation.html

From the Article: "Backslash Security has announced its launch with a new cloud-native application security (AppSec) solution designed to identify toxic code flows and automate threat models."

BrandPost: Stop the Sprawl: How Vendor Consolidation Can Reduce Security Risks in the Cloud

Source: https://www.csoonline.com/article/3689951/stop-the-sprawl-how-vendor-consolidation-can-reduce-security-risks-in-the-cloud.html

From the Article: "Managing multiple security vendors is proving to be a significant challenge for organizations, leading to difficulties in integration, visibility, and control. Recent surveys and reports have identified numerous problems associated with managing an assortment of security products from different vendors, and that managing multiple vendors was cited as the top challenge in achieving an effective security posture."

As critical Microsoft vulnerabilities drop, attackers may adopt new techniques

Source: https://www.csoonline.com/article/3691137/as-critical-microsoft-vulnerabilities-drop-attackers-may-adopt-new-techniques.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: "While the total number of recorded Microsoft vulnerabilities was higher in 2022 than ever before, the number of critical vulnerabilities declined to its lowest point, according to the latest Microsoft Vulnerability Report by BeyondTrust, released Tuesday."

Developed countries lag emerging markets in cybersecurity readiness

Source: https://www.csoonline.com/article/3691294/developed-countries-lag-emerging-markets-in-cybersecurity-readiness.html

From the Article: "Organizations in developed countries are not as prepared for cybersecurity incidents compared to those in developing countries, according to Cisco's Cybersecurity Readiness Index, released today."

9 attack surface discovery and management tools

Source: https://www.csoonline.com/article/3691110/9-attack-surface-discovery-and-management-tools.html

From the Article: "Cyber asset attack surface management (CAASM) or external attack surface management (EASM) solutions are designed to quantify the attack surface and minimize and harden it. "

BianLian ransomware group shifts focus to extortion

Source: https://www.csoonline.com/article/3691130/bianlian-ransomware-group-shifts-focus-to-extortion.html

From the Article: "Ransomware group BianLian has shifted the main focus of its attacks away from encrypting the files of its victims to focusing more on extortion as a means to extract payments, according to cybersecurity firm Redacted."

7 guidelines for identifying and mitigating AI-enabled phishing campaigns

Source: https://www.csoonline.com/article/3690418/7-guidelines-for-identifying-and-mitigating-ai-enabled-phishing-campaigns.html

From the Article: "The emergence of effective natural language processing tools such as ChatGPT means it's time to begin understanding how to harden against AI-enabled cyberattacks."

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.

Play ransomware gang hit Dutch shipping firm Royal Dirkzwager

Source: https://securityaffairs.com/143714/cyber-crime/play-ransomware-royal-dirkzwager.html

From the Article: "Dutch maritime logistics company Royal Dirkzwager suffered a ransomware attack, the company was hit by the Play ransomware gang."

Security Firm Rubrik breached by Clop gang through GoAnywhere Zero-Day exploitation

Source: https://securityaffairs.com/143512/cyber-crime/rubrik-breached-goanywhere-zero-day-exploitation.html

From the Article: "Data security firm Rubrik discloses a data breach, attackers exploited recent GoAnywhere zero-day to steal its data."

Chinese-linked hackers deployed the most zero-day vulnerabilities in 2022, researchers say

Source: https://cyberscoop.com/mandiant-zero-day-vulnerabilities-china/

From the Article: "Researchers at the threat intelligence firm Mandiant observed the use of 55 zero-day vulnerabilities in 2022. That's a decrease from 2021 — when researchers recorded a whopping 81 — but a figure that nonetheless represents an overall rise in recent years of hackers exploiting previously unknown software vulnerabilities, which are a potent tool for digital spies and cybercriminals."

Hacker tied to D.C. Health Link breach says attack 'born out of Russian patriotism'

Source: https://cyberscoop.com/dc-health-link-breach-russia-hacker-congress/

From the Article: "The data beach that has exposed sensitive health care information of nearly two dozen members of Congress and their families — putting them along with tens of thousands of Washington area residents at risk of identity theft and additional cyberattacks — is apparently the work of a patriotic Russian hacker seeking to inflict damage on U.S. politicians."

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.

Rural hospitals need help from feds to fight ransomware, witnesses tell lawmakers

Source: https://cyberscoop.com/rural-hospital-ransomware/

From the Article: "As ransomware attacks continue to pummel the U.S. health care sector, costing hospitals millions of dollars and exposing patient's sensitive medical records, rural hospitals are in dire need of assistance from the federal government, experts said Thursday during a Senate hearing."

Scammers target Cloudflare CEO with Silicon Valley Bank-themed spearphishing

Source: https://cyberscoop.com/silicon-valley-bank-spearphishing-cloudflare/

From the Article: "When Silicon Valley Bank collapsed last week, tech executives panicked. Without access to funds deposited with SVB, many were unsure they'd be able to pay bills or make payroll. Fear set in — and scammers pounced. "

The US cybersecurity strategy won't address today's threats with regulation alone

Source: https://cyberscoop.com/national-cybersecurity-strategy-regulation/

From the Article: "Plenty of "unidentified flying objects" have appeared in the news over the past several weeks, yet cybersecurity professionals will tell you that we don't need to look up to find a more daunting and real threat to national security."

CISA: Federal civilian agency hacked by nation-state and criminal hacking groups

Source: https://cyberscoop.com/cisa-federal-civilian-agency-hacked/

From the Article: "A nation-state hacking group and a criminal gang best known for card skimming had access to a federal civilian agency from August to January 2023, according to a Wednesday joint alert released by the Cybersecurity and Infrastructure Security Agency, the FBI and the Multi-State Information Sharing and Analysis Center."

Microsoft: Russian hackers may be readying new wave of destructive attacks

Source: https://cyberscoop.com/russian-hackers-ukraine-cyberattacks/

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: "Russian hackers linked with destructive malware attacks may be preparing for a new wave of strikes, researchers with Microsoft's Digital Threat Analysis Center said Wednesday."

10 top cyber security vulnerabilities that you can't ignore (2023)

Source: https://www.cybertalk.org/2023/03/22/10-top-cyber-security-vulnerabilities-that-you-cant-ignore-2023/

From the Article: "Welcome to the digital age, where everything from our personal information to the critical infrastructure of entire nations is stored and managed online. The value of the aforementioned data is immense and cyber criminals are eager to capitalize on ill-gotten gains."

Ransomware Gang BianLian Switches to Extortion as its Primary Goal

Source: https://www.cysecurity.news/2023/03/ransomware-gang-bianlian-switches-to.html

From the Article: "The BianLian gang has abandoned its strategy of encrypting files and demanding a ransom in favour of outright extortion. "

Cyber Scammers now Experimenting With QR Codes

Source: https://www.cysecurity.news/2023/03/cyber-scammers-now-experimenting-with.html

From the Article: "Microsoft started limiting macros in Office files by default in February 2022, making it more difficult for attackers to execute malicious code."

Hacker Gang Holds Amazon's Ring to Ransom

Source: https://www.cysecurity.news/2023/03/hacker-gang-holds-amazons-ring-to-ransom.html

From the Article: "Amazon's Ring, a popular brand of home security cameras, is facing

a major cybersecurity threat. The company has been targeted by a ransomware gang, which has threatened to release sensitive data about Ring's customers if the company does not pay up."

Home Security: Breaches and Ransomware Making it Impossible to Review Firms and Their Security

Source: https://www.cysecurity.news/2023/03/home-security-breaches-and-ransomware.html

From the Article: "The recent Ring home security ransomware incident and Eufy's insecure network has left numerous researchers and users wondering about the cyber safety these home security and surveillance firms possess."

The DEA Portal Hack was Perpetrated by Two Cybercriminals Last Year

Source: https://www.cysecurity.news/2023/03/the-dea-portal-hack-was-perpetrated-by.html

From the Article: "During the investigation into the hacking of the DEA portal in 2022, one of the young American men was accused of breaking in and stealing data from the site. The portal breach provided criminals with access to sensitive information because it was connected to 16 data repositories of federal law enforcement organizations. "

Rising Cyberattacks Increase Stress on Healthcare Industry

Source: https://www.cysecurity.news/2023/03/rising-cyberattacks-increase-stress-on.html

From the Article: "The health industry has recently come under increasing pressure to protect sensitive data from cyberattacks as these attacks become more frequent and sophisticated. Healthcare providers have been targeted by cybercriminals seeking to obtain sensitive patient data such as medical records and financial information."

EV Charging Stations Prone to Cyber Attacks : Indian Govt to Parliament

Source: https://www.cysecurity.news/2023/03/ev-charging-stations-prone-to-cyber.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: "Electric vehicle charging stations, like any other technological application, are vulnerable to cyber attacks and cyber security incidents, Indian Parliament was informed on Thursday. "

LockBit 3.0 Ransomware: Inside the Million Dollar Cyberthreat

Source: https://www.cysecurity.news/2023/03/lockbit-30-ransomware-inside-million.html

From the Article: "US government organizations have recently published a joint cybersecurity advisory stating the indicators of compromise (IoCs) and tactics, techniques and procedures (TTPs) linked with the malicious LockBit 3.0 ransomware. "

Lender Latitude Customer Records Were Hacked in a Cyberattack

Source: https://www.cysecurity.news/2023/03/lender-latitude-customer-records-were.html

From the Article: "Cyber-attacks on a finance company belonging to Latitude Financial that could have compromised the privacy of more than 300,000 people may have led to the breach of more than 300,000 people's data in New Zealand and Australia. "

10 Vulnerabilities Types to Focus On This Year

Source: https://www.darkreading.com/edge-articles/10-vulnerability-types-to-focus-on-this-year

From the Article: "A new Tech Insight report examines how the enterprise attack surface is expanding and how organizations must deal with vulnerabilities in emerging technologies."

Attackers Are Probing for Zero-Day Vulns in Edge Infrastructure Products

Source: https://www.darkreading.com/attacks-breaches/attackers-probing-zero-day-vulns-edge-infrastructure

From the Article: "Nearly 20% of the zero-day flaws that attackers exploited in 2022

Link back to Table of Contents

were in network, security, and IT management products, Mandiant says."

Pipeline Cybersecurity Rules Show the Need for Public-Private Partnerships

Source: https://www.darkreading.com/ics-ot/pipeline-cybersecurity-rules-show-the-need-for-public-private-partnerships

From the Article: "The government should not issue infrastructure regulations without the involvement of the industries it's regulating."

.NET Devs Targeted With Malicious NuGet Packages

Source: https://www.darkreading.com/application-security/net-devs-targeted-with-malicious-nuget-packages

From the Article: "In a possible first for the NuGet repository, more than a dozen components in the .NET code repository run a malicious script upon installation, with no warning or alert."

ChatGPT Gut Check: Cybersecurity Threats Overhyped or Not?

Source: https://www.darkreading.com/attacks-breaches/chatgpt-gut-check-openai-cybersecurity-threat-overhyped

From the Article: "UK cybersecurity authorities and researchers tamp down fears that ChatGPT will overwhelm current defenses, while the CEO of OpenAI worries about its use in cyberattacks."

Controlling Third-Party Data Risk Should Be a Top Cybersecurity Priority

Source: https://www.darkreading.com/attacks-breaches/controlling-third-party-data-risk-should-be-a-top-cybersecurity-priority-

From the Article: "Third-party breaches have a wide effect that legacy security practices can no longer detect."

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 Skills Shortage, Recession Fears Drive 'Upskilling' Training Trend

Source: https://www.darkreading.com/vulnerabilities-threats/cybersecurity-skills-shortage-recession-fears-drive-upskilling-training-trend

From the Article: "For companies, training an existing worker is cheaper than hiring, while for employees, training brings job security and more interesting work."

Re: Microsoft PlayReady security research

Source: https://seclists.org/fulldisclosure/2023/Mar/12

From the Article: "While Microsoft claims there is absolutely no bug at its end, I personally start to perceive the company as the one that should be also blamed to some extent."

Hackers Weaponized and Exploited Over 55 Zero-days in Microsoft, Google, and Apple

Source: https://gbhackers.com/55-zero-days/

From the Article: "Mandiant researchers have recently reported that 55 zero-day vulnerabilities were actively exploited in 2022, most against the following brands and their products:- Researchers state that hackers are still targeting zero-day vulnerabilities in malicious campaigns."

Activision Got Hacked but Didn't Tell Its Employees: Report

Source: https://gizmodo.com/activision-blizzard-call-duty-hacked-no-tell-employees-1850145082

From the Article: "This week, gaming giant Activision revealed that a cybercriminal had managed to get inside of its network late last year. How did the hacker do that, exactly? Better take a guess."

aCropalypse now! Cropped and redacted images suffer privacy fail on Google Pixel smartphones

Link back to Table of Contents

Source: https://www.bitdefender.com/blog/hotforsecurity/acropalypse-now-cropped-and-redacted-images-suffer-privacy-fail-on-google-pixel-smartphones/

From the Article: "Perhaps you've cropped out part of the image you didn't want others to see? Well, users of Google's Pixel Android smartphone might be alarmed to learn that pictures they've shared in the past may have been less discreet than they imagined."

New Android Botnet Nexus Being Rented Out on Russian Hacker Forum

Source: https://www.hackread.com/android-botnet-nexus-sold-russian-hacker-forum/

From the Article: "Nexus contains a module equipped with encryption capabilities which point towards ransomware."

Google Suspends Chinese Shopping App Pinduoduo Over Malware Concerns

Source: https://www.hackread.com/google-suspends-china-pinduoduo-app-malware/

From the Article: "Pinduoduo has confirmed the incident, but denied the presence of malware in its app."

Breach Forums to Remain Offline Permanently

Source: https://www.hackread.com/breach-forums-offline-permanently/

From the Article: "One of the Breach Forums administrators who goes by the alias Baphomet has decided to shut down the forum permanently."

DotRunpeX: The Malware That Infects Systems with Multiple Families

Source: https://www.hackread.com/dotrunpex-malware-infects-multiple-families/

From the Article: "Researchers suspect that the malware may be operated by Russian-speaking groups, given the references to the language in its code."

Link back to Table of Contents

Hackers can hijack Samsung and Pixel phones by knowing phone number

Source: https://www.hackread.com/hackers-hijack-samsung-pixel-phone-number/

From the Article: "In addition to Google Pixel and Samsung devices, Vivo devices were also vulnerable to this attack."

Threat Actors Use the MageCart Malware in New Credit Card Data Stealing Campaign

Source: https://heimdalsecurity.com/blog/threat-actors-use-the-magecart-malware-in-new-credit-card-data-stealing-campaign/

From the Article: "A new credit card hacking campaign is wreaking havoc, but this time it's a little bit different. Instead of injecting the JavaScript code into the HTML of the store or of the checkout pages, this time threat actors are hiding the malicious code inside the "Authorize.net" payment gateway module for WooCommerce."

New PowerMagic and CommonMagic Malware Used by Threat Actors to Steal Data

Source: https://heimdalsecurity.com/blog/new-powermagic-and-commonmagic-malware-used-by-threat-actors-to-steal-data/

From the Article: "A new backdoor dubbed PowerMagic and "a previously unseen malicious framework" named CommonMagic were utilized in assaults by an advanced threat actor, according to security researchers."

Researchers Reveal Insights into CatB Ransomware's Advanced Evasion Methods

Source: https://heimdalsecurity.com/blog/researchers-reveal-insights-into-catb-ransomwares-advanced-evasion-methods/

From the Article: "To avoid detection and launch of the payload, threat actors behind CatB ransomware used a technique called DLL search order hijacking. Based on code-level similarities, CatB, also known as CatB99 and Baxtoy, emerged late last year and is said to be an "evolution or direct rebrand" of another ransomware strain known as Pandora. "

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.

Banking Trojan Mispadu Found Responsible for 90,000+ Credentials Stolen

Source: https://heimdalsecurity.com/blog/banking-trojan-mispadu/

From the Article: "Multiple spam campaigns targeting Bolivia, Chile, Mexico, Peru, and Portugal have been linked to a banking trojan called Mispadu that steals credentials and delivers other malicious payloads."

A Cancer Patient's Fight for Justice Against a Hospital Ransomware Attack

Source: https://heimdalsecurity.com/blog/a-cancer-patients-fight-for-justice-against-a-hospital-ransomware-attack/

From the Article: "A cancer patient whose naked medical photos and records were stolen by a ransomware gang and posted online has sued her healthcare provider for allowing the "preventable" and "seriously damaging" data leak."

A closer look at TSA's new cybersecurity requirements for aviation

Source: https://www.helpnetsecurity.com/2023/03/23/aviation-industry-cybersecurity-requirements/

From the Article: "The Transportation Security Administration (TSA) recently issued new cybersecurity requirements for the aviation industry, which follows last year's announcement for railroad operators. "

Top 5 security risks for enterprise storage, backup devices

Source: https://www.helpnetsecurity.com/2023/03/23/backup-device-vulnerabilities/

From the Article: "An average enterprise storage and backup device has 14 vulnerabilities, three of which are high or critical risk that could present a significant compromise if exploited, according to Continuity."

Vumetric PTaaS platform simplifies cybersecurity assessments for organizations

Source: https://www.helpnetsecurity.com/2023/03/23/vumetric-ptaas-platform/

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: "Vumetric Cybersecurity has launched its Penetration Testing as-a-Service (PTaaS) platform, designed to simplify and modernize cybersecurity assessments for organizations of all sizes. "

Secureworks Security Posture Dashboard enables businesses to understand their cyber readiness

Source: https://www.helpnetsecurity.com/2023/03/23/secureworks-security-posture-dashboard/

From the Article: "Secureworks bolsters cyber resiliency with launch Of Security Posture Dashboard. Using the 600 billion security events Taegis analyzes daily, the Dashboard empowers customers to understand their cybersecurity posture and how resilient they would be in the face of a cyberattack."

Lightspin Remediation Hub helps users fix the cloud security threats

Source: https://www.helpnetsecurity.com/2023/03/23/lightspin-remediation-hub/

From the Article: "Lightspin launched the Remediation Hub as part of its cloud-native application protection platform (CNAPP) solution. An evolution of Lightspin's root cause analysis feature, the Remediation Hub provides users the ability to dynamically remediate the most critical cloud environment risks, at scale."

These 15 European startups are set to take the cybersecurity world by storm

Source: https://www.helpnetsecurity.com/2023/03/22/european-cybersecurity-google-startups/

From the Article: "Google has announced the startups chosen for its Cybersecurity Startups Growth Academy. The 15 selected startups are from eight countries and were chosen from over 120 applicants. "

Bridging the cybersecurity readiness gap in a hybrid world

Source: https://www.helpnetsecurity.com/2023/03/22/cybersecurity-readiness-gap/

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 mere 15% of organizations globally have the ‘mature’ level of readiness needed to be resilient against today’s modern cybersecurity risks, according to a Cisco report."

How to combat hardware Trojans by detecting microchip manipulations

Source: https://www.helpnetsecurity.com/2023/03/22/hardware-trojans-detecting-microchip-manipulations/

From the Article: "Not only do security vulnerabilities lurk within software, but they can also be embedded directly into hardware, leaving technical applications open to widespread attack."

F5’s multi-cloud networking capabilities simplify operations for distributed application deployments

Source: https://www.helpnetsecurity.com/2023/03/22/f5-multi-cloud-networking-capabilities/

From the Article: "F5 announced multi-cloud networking (MCN) capabilities to extend application and security services across one or more public clouds, hybrid deployments, native Kubernetes environments, and edge sites."

Threat actors are experimenting with QR codes

Source: https://www.helpnetsecurity.com/2023/03/21/qr-scan-scams/

From the Article: "Hackers are diversifying attack methods, including a surge in QR code phishing campaigns, according to HP. From February 2022, Microsoft began blocking macros in Office files by default, making it harder for attackers to run malicious code. "

ForgeRock Enterprise Connect Passwordless reduces the risk of password-based attacks

Source: https://www.helpnetsecurity.com/2023/03/21/forgerock-enterprise-connect-

Link back to Table of Contents

passwordless/

From the Article: "ForgeRock announced ForgeRock Enterprise Connect Passwordless, a new passwordless authentication solution that eliminates the need for users to interact with passwords inside large organizations."

Eurotech introduces cybersecurity-certified edge AI solutions

Source: https://www.helpnetsecurity.com/2023/03/21/eurotech-edge-servers/

From the Article: "Eurotech announced its newest edge servers with scalable, cybersecurity certified – AI capabilities. Cyber-threats have become endemic and severely expose states and businesses of all sizes to the risk of loss of data, interruption of services, and direct or indirect monetary impact. "

Most mid-sized businesses lack cybersecurity experts, incident response plans

Source: https://www.helpnetsecurity.com/2023/03/20/mid-sized-businesses-cybersecurity-challenges/

From the Article: "99% of all businesses across the United States and Canada are mid-sized businesses facing cybersecurity challenges, according to a Huntress report. Aimed to gain insights into organizational structure, resources and cybersecurity strategies, the results contextualize challenges across core functions including gaps in toolkits, planning, staffing, security awareness training and difficulty to secure cybersecurity insurance."

How ChatGPT is changing the cybersecurity game

Source: https://www.helpnetsecurity.com/2023/03/17/chatgpt-cybersecurity-potential/

From the Article: "The cybersecurity industry can leverage GPT-3 potential as a co-pilot to help defeat attackers, according to Sophos. The latest report details projects developed by Sophos X-Ops using GPT-3's large language models to simplify the search for malicious activity in datasets from security software, more accurately filter spam, and speed up analysis of "living off the land" binary (LOLBin) attacks."

Link back to Table of Contents

Perception Point adds DLP capabilities to detect, prevent, and remediate web threats

Source: https://www.helpnetsecurity.com/2023/03/17/perception-point-dlp/

From the Article: "Perception Point has added browser-centric Data Loss Prevention (DLP) capabilities to its Advanced Browser Security extension. The Browser Security plugin provides comprehensive security measures and granular controls to safeguard corporate assets from loss, misuse, and unauthorized access."

Amazon Linux 2023: Create and execute cloud-based applications with enhanced security

Source: https://www.helpnetsecurity.com/2023/03/16/amazon-linux-2023/

From the Article: "AWS has been offering Amazon Linux, a cloud-optimized Linux distribution, since 2010. This distribution's latest version is now available. Amazon Linux 2023 is provided at no additional charge. Standard Amazon EC2 and AWS charges apply for running EC2 instances and other services. This distribution includes full support for five years. "

Cyber attribution: Vigilance or distraction?

Source: https://www.helpnetsecurity.com/2023/03/16/cyber-attribution-vigilance-or-distraction/

From the Article: "Cyber attribution is a process by which security analysts collect evidence, build timelines and attempt to piece together evidence in the wake of a cyberattack to identify the responsible organization/individuals."

5 Key Components of Cybersecurity Hardening

Source: https://www.tripwire.com/state-of-security/key-components-cybersecurity-hardening

From the Article: "Hardening in Cybersecurity Cybersecurity hardening is a comprehensive approach to keeping your organization safe from intruders, and mitigating risk. By reducing your attack surface, vulnerability is reduced in tandem. "

Link back to Table of Contents

VIN Cybersecurity Exploits and How to Address Them in 2023

Source: https://www.tripwire.com/state-of-security/vin-cybersecurity-exploits-and-how-address-them

From the Article: "Cybersecurity is no longer the exclusive domain of computers, servers, and handheld devices. As wireless connectivity grows, it makes many daily activities more convenient, but it also means that cars may be vulnerable to cyberattacks. Connected, Autonomous, Shared and Electric vehicles are starting to dominate the auto market, but they often carry significant cybersecurity risks. "

Ransomware Risk Management: A Cybersecurity Framework Profile

Source: https://www.tripwire.com/state-of-security/ransomware-risk-management-cybersecurity-framework-profile

From the Article: "How big is Ransomware? The San Francisco 49ers, confirmed a ransomware attack, Cisco was attacked by the Yanluowang ransomware gang, and Entrust was attacked by Lockbit. "

Key Findings: UK Cybersecurity Breaches Survey 2022

Source: https://www.tripwire.com/state-of-security/key-findings-uk-cybersecurity-breaches-survey

From the Article: "The cybersecurity landscape is continuously evolving. It has led businesses to question how they are protecting themselves and their consumers from data breaches. "

Mandiant reveals hacktivists increasingly targeting OT systems, raising likelihood of actual and even substantial OT incidents

Source: https://industrialcyber.co/threat-landscape/mandiant-reveals-hacktivists-increasingly-targeting-ot-systems-raising-likelihood-of-actual-and-even-substantial-ot-incidents/

From the Article: "Threat intelligence firm Mandiant provided on Wednesday a comprehensive analysis of recent activity by hacktivists targeting OT (operational technology) systems, leveraging information from previously undisclosed and known

incidents to discuss the potential implications for OT defenders."

Winter Vivern APT group uses unknown set of espionage campaigns to strike government and private entities

Source: https://industrialcyber.co/ransomware/winter-vivern-apt-group-uses-unknown-set-of-espionage-campaigns-to-strike-government-and-private-entities/

From the Article: "SentinelLabs identified Winter Vivern APT (advanced persistent threat) activity, leveraging observations made by The Polish CBZC and Ukraine CERT. The hacker group employs various tactics, such as phishing websites, credential phishing, and deployment of malicious documents, tailored to the targeted organization's specific needs."

Waterfall's WF-600 unidirectional security gateway brings 'unbreachable protection' to OT/ICS networks

Source: https://industrialcyber.co/vendor/waterfalls-wf-600-unidirectional-security-gateway-brings-unbreachable-protection-to-ot-ics-networks/

From the Article: "OT security company Waterfall Security Solutions released on Monday its WF-600 unidirectional security gateway that blends hardware and software, enabling unbreachable protection at IT/OT interfaces with unlimited visibility into OT (operational technology) networks, systems, and data."

Homeland Security Committee convenes hearing to scrutinize cybersecurity risks to healthcare sector

Source: https://industrialcyber.co/medical/homeland-security-committee-convenes-hearing-to-scrutinize-cybersecurity-risks-to-healthcare-sector/

From the Article: "The Homeland Security and Governmental Affairs Committee convened a hearing to examine cybersecurity threats facing the healthcare sector and how the federal government and healthcare providers are working to prevent breaches."

Mandiant Zero-Day Exploitation Report 2022

Link back to Table of Contents

Source: https://informationsecuritybuzz.com/mandiant-zero-day-report-2022/

From the Article: "This report shares key findings from the Mandiant zero-day exploitation investigation of 2022. A zero-day vulnerability, according to Mandiant, is one that was used in the real world before a fix was made available."

Royal Dirkzwager Attacked By Play Ransomware Group

Source: https://informationsecuritybuzz.com/royal-dirkzwager-attacked-play-ransomware/

From the Article: "The Play ransomware group's campaign, the most recent in a succession of strikes on the shipping sector, was proven to have affected the Dutch marine transport company Royal Dirkzwager."

What Is Shoulder Surfing? How Does It Affect Cybersecurity

Source: https://informationsecuritybuzz.com/shoulder-surfing-affect-cybersecurity/

From the Article: "We rely primarily on technology to protect our sensitive data, including financial information, personal information, and corporate secrets, in the extremely digital world we live in today."

China-Aligned "Operation Tainted Love" Targets Middle East Telecom Providers

Source: https://www.infosecurity-magazine.com/news/operation-tainted-love-targets/

From the Article: "The deployment of custom credential theft malware is the main novelty of the new campaign."

SharePoint Phishing Scam Targets 1600 Across US, Europe

Source: https://www.infosecurity-magazine.com/news/sharepoint-phishing-scam-targets/

From the Article: "Cyber-criminals used the scam to steal the credentials for various email accounts."

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.

UK Government Sets Out Vision for NHS Cybersecurity

Source: https://www.infosecurity-magazine.com/news/government-sets-out-vision-nhs/

From the Article: "Plans to boost cyber-resilience in the health service by 2030."

Ransomware Attacks Double in Europe's Transport Sector

Source: https://www.infosecurity-magazine.com/news/ransomware-double-europes/

From the Article: "ENISA claims most threats are opportunistic."

Security Researchers Spot $36m BEC Attack

Source: https://www.infosecurity-magazine.com/news/security-researchers-spot-36m-bec/

From the Article: "Threat actors impersonated target company's vendor."

Hackers Use NuGet Packages to Target .NET Developers

Source: https://www.infosecurity-magazine.com/news/hackers-target-net-developers/

From the Article: "JFrog said this is the first instance of packages with malicious code in NuGet."

KillNet Group Uses DDoS Attacks Against Azure-Based Healthcare Apps

Source: https://www.infosecurity-magazine.com/news/killnet-ddos-healthcare-apps/

From the Article: "Microsoft said it saw between 40 and 60 daily attacks in February."

UK Ransomware Incident Volumes Surge 17% in 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://www.infosecurity-magazine.com/news/uk-ransomware-incident-surge-17/

From the Article: "Jumpsec report identified Karakurt, Lockbit and Vice Society among groups responsible."

"Hinata" Botnet Could Launch Massive DDoS Attacks

Source: https://www.infosecurity-magazine.com/news/hinata-botnet-could-launch-ddos/

From the Article: "Akamai warns of new Mirai-like botnet written in Go."

Telegram, WhatsApp Trojanized to Target Cryptocurrency Wallets

Source: https://www.infosecurity-magazine.com/news/telegram-whatsapp-trojanized/

From the Article: "Most of these apps rely on clipper malware to steal the contents of the Android clipboard."

Fortune 500 Company Names Found in Compromised Password Data

Source: https://www.itsecurityguru.org/2023/03/23/fortune-500-names-found-in-compromised-password-data/

From the Article: "New research released by Specops Software outlines the most common Fortune 500 company names that show up in compromised password data. The Specops research team analysed an 800 million password subset of the larger Breached Password Protection database to obtain these results. "

How Emerging Trends in Virtual Reality Impact Cybersecurity

Source: https://www.itsecurityguru.org/2023/03/21/how-emerging-trends-in-virtual-reality-impact-cybersecurity/

From the Article: "As information technology continues to evolve, more and more people are penetrating cyberspace. Most organizations, companies, individuals, and even governments are now doing their activities in the digital world. This allows them to enjoy

great benefits such as instant access from anywhere, less usage costs, and worldwide reach."

Phishing through SharePoint | Kaspersky official blog

Source: https://www.kaspersky.com/blog/sharepoint-notification-scam/47593/

From the Article: "A phishing link in the e-mail body is a thing of the past. Mail filters now detect this trick with near 100% efficiency. That's why cybercriminals are constantly inventing new ways to get their hands on corporate login credentials."

[Security Masterminds] Unlock Maximum Cybersecurity: 3 Crucial Steps to Enhance Your Capabilities, Coverage, and Culture

Source: https://blog.knowbe4.com/security-masterminds-enhance-capabilities-coverage-culture

From the Article: "Do you ever feel like you are always playing catch up regarding cybersecurity? That it is a never-ending game; no matter what you do, you are always one step behind."

Users Clicking on Multiple Mobile Phishing Links Increases 637% in Just Two Years

Source: https://blog.knowbe4.com/users-click-multiple-mobile-phishing-links

From the Article: "New data shows that phishing mobile devices as an attack vector is growing in popularity – mostly because it's increasingly working."

Identifying AI-Enabled Phishing

Source: https://blog.knowbe4.com/identifying-ai-enabled-phishing

From the Article: "Users need to adapt to an evolving threat landscape in which attackers can use AI tools like ChatGPT to craft extremely convincing phishing emails, according to Matthew Tyson at CSO."

Link back to Table of Contents

Half of Organizations Report at Least Monthly Outages from Cyberattacks

Source: https://blog.knowbe4.com/monthly-outages-from-cyberattacks

From the Article: "New data on the current state of cybersecurity shows that organizations are experiencing challenges, falling behind, and seeing the impact of all this post-attack."

Report Shows Business Email Compromise (BEC) Attacks Increase and Phishing Used as Initial Attack Vector in the Last Year

Source: https://blog.knowbe4.com/business-email-compromise-phishing-attacks-increase

From the Article: "Secureworks has published a report looking at cybercrime over the course of 2022, finding that business email compromise (BEC) attacks nearly doubled last year."

A 240% Rise in Dynamic Phishing

Source: https://blog.knowbe4.com/a-240-rise-in-dynamic-phishing

From the Article: "Attackers are increasingly using techniques to prevent their phishing pages from being detected by security firms, a new report from BlueVoyant has found."

92% of Organizations Have Fallen Victim to Phishing as Nearly Every Org is Concerned with Email Security

Source: https://blog.knowbe4.com/92-percent-organizations-phishing-victims

From the Article: "New data shows that not only has just about every organization experienced a successful phishing attack, but that they are also paying the price in a number of impactful ways."

Google Suspends Chinese E-Commerce App Pinduoduo Over Malware

Source: https://krebsonsecurity.com/2023/03/google-suspends-chinese-e-commerce-app-pinduoduo-over-malware/

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 says it has suspended the app for the Chinese e-commerce giant Pinduoduo after malware was found in versions of the software. The move comes just weeks after Chinese security researchers published an analysis suggesting the popular e-commerce app sought to seize total control over affected devices by exploiting multiple security vulnerabilities in a variety of Android-based smartphones."

CASPER Attack Targets Air-Gapped Systems Via Internal Speakers

Source: https://latesthackingnews.com/2023/03/21/casper-attack-targets-air-gapped-systems-via-internal-speakers/

From the Article: "Researchers have found another way that potentially risks the security of air-gapped systems. "

ROHM's ultra-high-speed control IC technology maximizes performance of GaN switching devices

Source: https://www.semiconductor-today.com/news_items/2023/mar/rohm-230323.shtml

From the Article: "Due to their superior high-speed switching characteristics the adoption of GaN devices has expanded in recent years. "

Unknown Actors Deploy Malware To Steal Data In Occupied Regions Of Ukraine

Source: https://www.theregister.com/2023/03/22/commonmagic_kaspersky_espionage_ukraine/

From the Article: "A cyber espionage campaign targeting organizations in Russian-occupied regions of Ukraine is using novel malware to steal data, according to Russia-based infosec software vendor Kaspersky."

Malware creator who compromised 10,000 computers arrested

Source: https://www.malwarebytes.com/blog/news/2023/03/creator-of-rat-disguised-as-fake-game-application-arrested

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: "Once data was harvested by the RAT, some of it was put to further use: Account theft and withdrawal of electronic funds contained in compromised balances are both mentioned in the police release."

Google reveals 18 chip vulnerabilities threatening mobile, wearables, vehicles

Source: https://www.malwarebytes.com/blog/news/2023/03/google-reveals-18-chip-vulnerabilities-threatening-mobile-wearables-vehicles

From the Article: "Google's Project Zero is warning of multiple significant vulnerabilities found across many models of mobile devices including Samsung Galaxy, Google Pixel, Vivo, and several forms of wearable and vehicles using certain types of components."

The Future of Cyber is Automated Moving Target Defense—Gartner

Source: https://blog.morphisec.com/automated-moving-target-defense-gartner

From the Article: "Gartner® has published a new report focused onAutomated Moving Target Defense (AMTD) technology."

Windows 11 also vulnerable to "aCropalypse" image data leakage

Source: https://nakedsecurity.sophos.com/2023/03/22/windows-11-also-vulnerable-to-acropalypse-image-data-leakage/

From the Article: "Turns out that the Windows 11 Snipping Tool has the same "aCropalypse" data leakage bug as Pixel phones."

Collaboration Over Self-Preservation Highlighted in Latest Guide to Cyber Oversight

Source: https://www.nextgov.com/cybersecurity/2023/03/collaboration-over-self-preservation-highlighted-latest-guide-cyber-oversight/384375/

From the Article: "CISA Director Jen Easterly said that the updated cyber-risk oversight handbook aligns with the agency's goal of "advancing corporate cyber responsibility.""

Link back to Table of Contents

Lawmakers Propose Civilian Cyber Reserve to Bolster DOD and DHS

Source: https://www.nextgov.com/cybersecurity/2023/03/lawmakers-propose-civilian-cyber-reserve-bolster-dod-and-dhs/384273/

From the Article: "The bipartisan package of two bills would address the government's shortage of skilled cyber personnel by allowing DOD and DHS "to recruit qualified civilian cybersecurity personnel to serve in reserve capacities.""

Senators Request Cyber Safety Analysis of Chinese-Owned DJI Drones

Source: https://www.nextgov.com/cybersecurity/2023/03/senators-request-cyber-safety-analysis-chinese-owned-dji-drones/384211/

From the Article: "Lawmakers raised concerns that sensitive data could leak to adversaries through foreign-owned consumer technology."

CISA: Election Security Still Under Threat at Cyber and Physical Level

Source: https://www.nextgov.com/cybersecurity/2023/03/cisa-election-security-still-under-threat-cyber-and-physical-level/384172/

From the Article: "Threats enacted by state-sponsored actors during the 2022 election have highlighted the need for "continued vigilance" in upcoming elections, said CISA Election Security Advisor Kim Wyman."

Threat Actor Attempted Email Compromise Attack For $36 Million

Source: https://www.scmagazine.com/news/email-security/threat-actor-vendor-email-compromise-attack-36-million

From the Article: "A vendor email compromise (VEC) attack that sought to change bank account information on a third-party insurance company's escrow account and pay a dummy title insurance company a $36 million invoice was recently discovered, pointing out the need for constant vigilance and increased training."

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.

What Is The Microsoft Print Spooler Vulnerability?

Source: https://packetstormsecurity.com/news/view/34442/What-Is-The-Microsoft-Print-Spooler-Vulnerability.html

From the Article: "You may not think of printers as targets for hackers. Unfortunately, though, cybercriminals can, and often do, exploit vulnerabilities associated with them. One of the more recent instances came from a Microsoft Print Spooler vulnerability that people nicknamed PrintNightmare. Cybersecurity researchers discovered it in March 2021. "

Inside The DEA Tool Hackers Allegedly Used To Extort Targets

Source: https://www.vice.com/en/article/z3mexy/inside-the-dea-tool-hackers-allegedly-used-extort-epic-portal

From the Article: "Hackers accused of using law enforcement tools and other tactics to extort people online gained access to a sensitive, password protected portal run by the Drug Enforcement Administration, according to a screenshot of the portal obtained by Motherboard."

The FBI Warns SIM Swapping Attacks Are Rising. What's That?

Source: https://packetstormsecurity.com/news/view/34435/The-FBI-Warns-SIM-Swapping-Attacks-Are-Rising.-Whats-That.html

From the Article: "In February 2022, the Federal Bureau of Investigation (FBI) issued Alert Number I-020822-PSA. It's entitled "Criminals Increasing SIM Swap Schemes to Steal Millions of Dollars from US Public" and it comes amid a general increase in cybercrime across the globe."

Bad Actors Exploited RCE In Progress Telerik To Hack US Agency

Source: https://www.scmagazine.com/news/threat-intelligence/bad-actors-exploited-rce-in-progress-telerik-to-hack-us-agency-server

From the Article: "Multiple cyber threat actors exploited a vulnerability that was first documented in 2019 that allows remote code execution (RCE) to access a federal agency's web server over a roughly three-month period, the U.S. Cybersecurity and

Infrastructure Agency reported."

Data Protection Vendor Acronis Admits To Data Leak As 12GB Trove Appears Online

Source: https://www.theregister.com/2023/03/10/acronis_data_breach/

From the Article: "The CISO of Acronis has downplayed what appeared to be an intrusion into its systems, insisting only one customer was affected, using stolen credentials, and that all other data remains safe."

DarkTrace Warns Of Rise In AI-Enhanced Scams Since ChatGPT Release

Source: https://www.theguardian.com/technology/2023/mar/08/darktrace-warns-of-rise-in-ai-enhanced-scams-since-chatgpt-release

From the Article: "The cybersecurity firm Darktrace has warned that since the release of ChatGPT it has seen an increase in criminals using artificial intelligence to create more sophisticated scams to con employees and hack into businesses."

Cryptocurrency Scams: What to Know and How to Avoid Them

Source: https://www.pandasecurity.com/en/mediacenter/security/cryptocurrency-scams/

From the Article: "Hackers are going to hack, and scammers are going to scam — no matter how much technology changes. While cryptocurrency is a new and exciting investment opportunity, it is vulnerable to cryptocurrency scams."

ACSC Essential 8 Cybersecurity Strategies, Maturity Levels, and Best Practices

Source: https://blog.qualys.com/vulnerabilities-threat-research/2023/03/21/acsc-essential-8-cybersecurity-strategies-maturity-levels-and-best-practices

From the Article: "Originally published in 2017 as an evolution of the Australian Signals Directorate's Strategies to Mitigate Cyber Security Incidents, the Australian Cyber Security Centre (ACSC) Essential 8 (E8) consists of a set of strategies that can make it harder for threat actors to compromise a firm's cybersecurity defenses. "

Link back to Table of Contents

A New Approach to Discover, Monitor, and Reduce Your Modern Web Attack Surface

Source: https://blog.qualys.com/product-tech/2023/03/16/a-new-approach-to-discover-monitor-and-reduce-your-modern-web-attack-surface

From the Article: "Web applications reign the internet universe, but also bring new risks that let attackers poke holes in an ever-expanding attack surface. Stolen credentials have been the historical culprit."

Radware Customers Share Their Personal Ransomware Story

Source: https://blog.radware.com/all/customer-corner/2023/03/radware-customers-share-their-ransomware-story/

From the Article: "Just the word ransom lets you know that ransomware isn't a welcome visitor. No industry is immune to it. In fact, many attacks on healthcare systems have prevented patients from getting medical care."

Threat Intelligence Feeds for Better DDoS Protection

Source: https://blog.radware.com/security/2023/03/threat-intelligence-feeds-for-better-ddos-protection/

From the Article: "DDoS (distributed denial of service) attacks have become a major threat to a huge variety of businesses, from the smallest to the largest multi-national corporations. "

From Ransomware to Cyber Espionage: 55 Zero-Day Vulnerabilities Weaponized in 2022

Source: https://thehackernews.com/2023/03/from-ransomware-to-cyber-espionage-55.html

From the Article: "As many as 55 zero-day vulnerabilities were exploited in the wild in 2022, with most of the flaws discovered in software from Microsoft, Google, and Apple."

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.

Ransomware Attacks Machinery Often Works on Russian Power - Truthmeter

Source: https://truthmeter.mk/ransomware-attacks-machinery-often-works-on-russian-power/

From the Article: "Russia has been denying for years that is a host of the hackers behind ransomware attacks, but cybersecurity experts claim there is evidence that many of these criminal groups are coordinated from this country."

Ransomware surges as threat actors get more aggressive - BetaNews

Source: https://betanews.com/2023/03/21/ransomware-surges-as-threat-actors-get-more-aggressive/

From the Article: "Ransomware and extortion actors are utilizing more aggressive tactics to pressure organizations, with harassment being involved 20 times more often than in 2021, according to a new report."

Palo Alto Networks report finds ransomware groups using heavy-handed tactics to force payments

Source: https://insidecybersecurity.com/daily-news/palo-alto-networks-report-finds-ransomware-groups-using-heavy-handed-tactics-force

From the Article: "A new report by Palo Alto Networks' Unit 42 threat intelligence team finds ransomware threat actors are increasingly using harassment tactics to pry money out of victims, while also finding "spikes" in attacks on schools and hospitals "demonstrating how low these actors are willing to stoop in their attacks.""

Hackers increasingly use phone and email harassment to extort ransom payments

Source: https://siliconangle.com/2023/03/21/hackers-increasingly-use-phone-email-harassment-extort-ransom-payments/

From the Article: "A new report out today from Palo Alto Networks Inc.'s Unit 42 finds that ransomware and extortion actors are using more aggressive tactics to pressure organizations, with harassment involved 20 times more often in ransomware attacks than in 2021."

Link back to Table of Contents

Ransomware gangs harass victims to 'bypass' backups - Computer Weekly

Source: https://www.computerweekly.com/news/365532726/Ransomware-gangs-harass-victims-to-bypass-backups

From the Article: "Ransomware gangs are becoming increasingly assertive and aggressive in their approaches to victims, resorting to high-pressure tactics including campaigns of targeted harassment to extort money, even from those that have paid attention to ransomware prevention and maintain backups of their data."

Privacy Consultant Calls Hive Ransomware "Sophisticated Operation" - VOCM

Source: https://vocm.com/2023/03/20/ransomware-attack-hive/

From the Article: "A local privacy consultant says Hive Ransomware, the group behind the cyberattack on the province's health care system, was a sophisticated operation, now dismantled by the FBI and US Department of Justice."

Royal Dirkzwager Attacked By Play Ransomware Group - Information Security Buzz

Source: https://informationsecuritybuzz.com/royal-dirkzwager-attacked-play-ransomware/

From the Article: "The Play ransomware group's campaign, the most recent in a succession of strikes on the shipping sector, was proven to have affected the Dutch marine transport company Royal Dirkzwager. The company's CEO, Joan Blaas, who acquired it in October after it declared bankruptcy the previous month, told The Record that the ransomware attack did not affect business operations. But it resulted in data theft from servers that housed various contracts and individual data."

After a free decryptor is discovered, the BianLian ransomware crew goes 100% extortion

Source: https://www.bollyinside.com/news/technology/after-a-free-decryptor-is-discovered-the-bianlian-ransomware-crew-goes-100-extortion/

From the Article: "Cybersecurity firm Avast released a free decryptor in January to BianLian victims that apparently convinced the crooks that there was no future for them

Link back to Table of Contents

on the ransomware side and that extortion was outright."

CISA, FBI, MS-ISAC Warn Critical Infrastructure of LockBit 3.0 Ransomware Attacks

Source: https://healthitsecurity.com/news/cisa-fbi-ms-isac-warn-critical-infrastructure-of-lockbit-3.0-ransomware-attacks

From the Article: "LockBit 3.0 ransomware operations as a RaaS model and is known to attack a wide range of sectors, including those in critical infrastructure."

SpaceX Third Party Vendor Hit by LockBit Ransomware, Gang Claims That It Stole ...

Source: https://www.cpomagazine.com/cyber-security/spacex-third-party-vendor-hit-by-lockbit-ransomware-gang-claims-that-it-stole-engineering-schematics/

From the Article: "Elon Musk is in the news once again, but this time as the victim of a crime. The LockBit ransomware group claims that it was able to penetrate SpaceX via a third party vendor, and is holding design documents that it is threatening to sell to the aerospace pioneer's competitors."

Customer data exposed in a ransomware attack - Gearrice

Source: https://www.gearrice.com/update/customer-data-exposed-in-a-ransomware-attack/

From the Article: "The Prancing Horse firm has just been the victim of a cyberattack through what is known as ransomware or data hijacking. The company has sent a letter to its customers informing them of the details and explaining that some sensitive data such as name, surname, postal address, email or mobile phone number of customers have been seen exposed."

Ransomware Protection Market Size, Trends, Latest Techniques, Key Segments ... - Taiwan News

Source: https://www.taiwannews.com.tw/en/news/4841378

From the Article: "The recent analysis by Report Ocean on the global Ransomware

Protection Market Report 2021 revolves around various aspects of the market, including characteristics, size and growth, segmentation, regional and country breakdowns, competitive landscape, market shares, trends, strategies, etc."

BECs Double In 2022, Overtaking Ransomware - TechRepublic

Source: https://www.techrepublic.com/article/business-email-compromises-double-overtake-ransomware/

From the Article: "A look at 4th quarter 2022, data suggests that new threat surfaces notwithstanding, low-code cybersecurity business email compromises including phishing, as well as MFA bombing are still the prevalent exploits favored by threat actors."

ivinsvu - what kind of ransomware is this? - Bleeping Computer

Source: https://www.bleepingcomputer.com/forums/t/783546/ivinsvu-what-kind-of-ransomware-is-this/

From the Article: "This is Magniber Ransomware 2022 which will have a 7-10 random character extension (.cyvpbwzfv, .lpdyefulm, .yyqiidt, .hihxhgx, .zxvdfcyyz, .giapk33vw, .kjidvyteg, .oepyvjuox) appended to the end of the encrypted data filename and typically will leave files (ransom notes) named README.html, README.txt."

Facing up to the cyber threat - Business Plus

Source: https://businessplus.ie/tech/cyber-threat/

From the Article: "Cyber security specialist Kroll's latest Threat Landscape Report has warned that ransomware attacks rebounded strongly in Q4 2022, with a significant spike in focus on technology and manufacturing. Not only have familiar threats not gone away, but they continue to evolve and adapt."

New Trigona ransomware strain up and running, but still evolving - Cyber Security Connect

Source: https://www.cybersecurityconnect.com.au/technology/8814-new-trigona-

Link back to Table of Contents

ransomware-strain-up-and-running-but-still-evolving

From the Article: "Security researchers have identified a new strain of ransomware in operation and that it is undergoing active development in the wild."

Changing Cyber Landscape Poses Challenges For Health-Care Market - Insurance Journal

Source: https://www.insurancejournal.com/magazines/mag-features/2023/03/20/712578.htm

From the Article: "If you've sold a cyber liability insurance policy lately, you know how quickly the market has evolved. Policies that were once inexpensive and universally available are now high-priced and hard to find."

New Cybersecurity approaches for staying ahead of threats - SecurityBrief Australia

Source: https://itbrief.com.au/story/new-cybersecurity-approaches-for-staying-ahead-of-threats

From the Article: "This year, we will see a significant rise in data breaches that will directly impact everyday life as the scale of cyber threats grows, spilling into the mainstream. Threat actors will look to exploit vulnerabilities in Internet of Things (IoT)-enabled devices as the remarkable growth of connected devices continues to dominate the market."

BianLian Ransomware Crew Ditches Ransom Upon Encryption to Full-On Extortion - Tech Times

Source: https://www.techtimes.com/articles/289227/20230319/bianlian-ransomware-crew-ditches-ransom-upon-encryption-to-full-on-extortion-no-more-free-decryptor-victims.htm

From the Article: "As ransomware continues to be a major problem for organizations and victims alike, one group of cybercriminals is changing its tactics. The BianLian group is shifting from encrypting files and demanding a ransom to a model of pure extortion. "

Link back to Table of Contents

The Effect of the Ransomware Dataset Age on the Detection Accuracy of Machine Learning Models

Source: https://www.mdpi.com/2078-2489/14/3/193

From the Article: "The rapid development of computer networks and technology has led to the exposure of smartphone functionalities, which are provided by different applications and operating systems. "

Check Point finds potential cybercrime scenarios in ChatGPT4 - SecurityBrief Australia

Source: https://securitybrief.co.uk/story/check-point-finds-potential-cybercrime-scenarios-in-chatgpt4

From the Article: "Check Point Research (CPR) has released an initial analysis of ChatGPT4, surfacing five scenarios that allow threat actors to streamline malicious efforts and preparations faster and more precisely."

ACSC Ransomware Profile – Lockbit 3.0 | The National Tribune

Source: https://www.nationaltribune.com.au/acsc-ransomware-profile-lockbit-30/

From the Article: "The Australian Cyber Security Centre (ACSC) is aware of Lockbit 3.0 which is the newest version of Lockbit ransomware."

Business email compromises overtake ransomware as cybercrime of choice - SecurityBrief Asia

Source: https://itbrief.co.nz/story/bec-overtakes-ransomware-as-cybercrime-of-choice

From the Article: "With talk of advanced AI-driven threats dominating the cybersecurity industry, new research by the Secureworks Counter Threat Unit has revealed that most real-world security incidents have more humble beginnings highlighting a need for businesses to focus on cyber hygiene to bolster their network defences."

New SILKLOADER malware loader gains traction in Russian, Chinese hackers | SC Media

Source: https://www.scmagazine.com/brief/ransomware/new-silkloader-malware-loader-

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.

gains-traction-in-russian-chinese-hackers

From the Article: "Tap, tap - is this thing on? Why do defenders still struggle to detect attacks and attacker activities? Why do so many tools struggle to detect attacks? Today, we've got an expert on detection engineering to help us answer these questions."

Lawmakers are sounding the alarm after recent cyber attacks at hospitals - WSB-TV

Source: https://www.wsbtv.com/news/washington-news-bureau/lawmakers-are-sounding-alarm-after-recent-cyber-attacks-hospitals/Q7ZHBQGGHRBMPISXAAM44AN254/

From the Article: "Lawmakers in Washington say they're happening more frequently and they held a hearing to address what needs to happen."

It's impossible to review security cameras in the age of breaches and ransomware

Source: https://www.androidcentral.com/accessories/smart-home/its-impossible-to-review-security-cameras-in-the-age-of-breaches-and-ransomware

From the Article: "I've been waiting for the right time to review some old indoor security cameras for the past several months. It's not about the brand (Blink) or the cameras (which work quite well thus far!)."

Pro-Russia hackers are increasingly targeting hospitals, researchers warns

Source: https://therecord.media/killnet-ddos-hospitals-healthcare-russia

From the Article: "Cybersecurity researchers said this week that they have observed the pro-Russia hacking group known as Killnet increasingly launch distributed denial of service (DDoS) attacks targeting healthcare organizations since November."

MONTI ransomware gang leaks Donut Leaks - DataBreaches.net

Source: https://www.databreaches.net/monti-ransomware-gang-leaks-donut-leaks/

Link back to Table of Contents

From the Article: "In one of the more intriguing listings of this week, the MONTI ransomware group has added another group, Donut Leaks, to their leak site."

Rubrik Confirms Attack via GoAnywhere Zero-Day Exploit: Over 130 Organizations Targeted ...

Source: https://techpresident.com/rubrik-confirms-attack-via-goanywhere-zero-day-exploit-over-130-organizations-targeted-by-cl0p-ransomware-group/

From the Article: "In this article, we'll look at the reasons behind the GoAnywhere zero-day exploit targeting data security firm Rubrik and its far-reaching implications for the cybersecurity industry. "

Russian Sanctions Evasion Puts Merchants and Banks at Risk

Source: https://www.recordedfuture.com/russian-sanctions-evasion-puts-merchants-banks-risk

From the Article: "Cybercriminals devise and execute various workarounds to legalize their illicit income. After international sanctions were leveled against Russia in the wake of Russias full-scale invasion of Ukraine, ordinary Russian consumers have likely resorted to similar workarounds to obtain goods produced abroad."

Improve your cyber threat coverage with Microsoft E5

Source: https://redcanary.com/blog/microsoft-e5-security-features/

From the Article: "E5 is the premier licensing tier for Microsoft's software-as-a-service (SaaS) products. Put simply, the E5 licensing tier grants customers access to more product entitlements, or "workloads," than Microsoft's other enterprise licensing tiers, E1 and E3."

Threat Hunting: The Intel Needle in the Haystack

Source: https://www.reliaquest.com/blog/threat-hunting-threat-intelligence/

From the Article: "A great threat hunt is fueled by a solid understanding of your

business, the associated risks, and the methods attackers are using to access your environment. It all starts with identifying meaningful threat intelligence and using it to produce valuable threat-hunting topics that are relevant to your environment."

Experts published PoC exploit code for Veeam Backup & Replication bug

Source: https://securityaffairs.com/143930/hacking/veeam-backup-replication-poc-exploit.html

From the Article: "Researchers released a PoC exploit code for a high-severity vulnerability in Veeam Backup & Replication (VBR) software."

Experts released PoC exploits for severe flaws in Netgear Orbi routers

Source: https://securityaffairs.com/143863/hacking/netgear-orbi-routers-flaws.html

From the Article: "Netgear Orbi is a line of mesh Wi-Fi systems designed to provide high-speed, reliable Wi-Fi coverage throughout a home or business. The Orbi system consists of a main router and one or more satellite units that work together to create a seamless Wi-Fi network that can cover a large area with consistent, high-speed Wi-Fi."

Independent Living Systems data breach impacts more than 4M individuals

Source: https://securityaffairs.com/143832/data-breach/independent-living-systems-data-breach.html

From the Article: "US health services company Independent Living Systems (ILS) disclosed a data breach that exposed personal and medical information for more than 4 million individuals."

New Bad Magic APT used CommonMagic framework in the area of Russo-Ukrainian conflict

Source: https://securityaffairs.com/143816/apt/apt-uses-commonmagic-framework.html

From the Article: "Threat actors are targeting organizations located in Donetsk, Lugansk, and Crimea with a previously undetected framework dubbed CommonMagic."

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.

Acropalypse flaw in Google Pixel's Markup tool allowed the recovery of edited images

Source: https://securityaffairs.com/143748/hacking/google-pixel-acropalypse-flaw.html

From the Article: "Security researchers Simon Aarons and David Buchanan have discovered a vulnerability, named 'Acropalypse,' in the Markup tool of Google Pixel. The Markup tool is a built-in Markup utility, released with Android 9 Pie that allows Google Pixel users to edit (crop, add text, draw, and highlight) screenshots."

Play ransomware gang hit Dutch shipping firm Royal Dirkzwager

Source: https://securityaffairs.com/143714/cyber-crime/play-ransomware-royal-dirkzwager.html

From the Article: "Royal Dirkzwager is specialized in optimizing shipping processes and managing maritime and logistic information flows."

Cybersecurity 101: What is Attack Surface Management?

Source: https://securityintelligence.com/cybersecurity-101-what-is-attack-surface-management/

From the Article: "There were over 4,100 publicly disclosed data breaches in 2022, exposing about 22 billion records. Criminals can use stolen data for identity theft, financial fraud or to launch ransomware attacks. While these threats loom large on the horizon, attack surface management (ASM) seeks to combat them."

The Role of Finance Departments in Cybersecurity

Source: https://securityintelligence.com/articles/role-finance-departments-cybersecurity/

From the Article: "Consumers are becoming more aware of the data companies collect about them, and place high importance on data security and privacy. Though consumers aren't aware of every data breach, they are justifiably concerned about what happens to the data companies collect. "

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.

Analysis: SEC Cybersecurity Proposals and Biden's National Cybersecurity Strategy

Source: https://www.securityweek.com/analysis-sec-cybersecurity-proposals-and-bidens-national-cybersecurity-strategy/

From the Article: "On March 15, 2023, the SEC announced a proposal for new cybersecurity requirements for covered entities."

Intel Boasts Attack Surface Reduction With New 13th Gen Core vPro Platform

Source: https://www.securityweek.com/intel-boasts-attack-surface-reduction-with-new-13th-gen-core-vpro-platform/

From the Article: "Intel's newest vPro platform brings threat prevention features with dozens of security capabilities built into the silicon."

Tackling the Challenge of Actionable Intelligence Through Context

Source: https://www.securityweek.com/tackling-the-challenge-of-actionable-intelligence-through-context/

From the Article: "Making threat intelligence actionable requires more than automation; it also requires contextualization and prioritization."

High-Severity Vulnerabilities Found in WellinTech Industrial Data Historian

Source: https://www.securityweek.com/high-severity-vulnerabilities-found-in-wellintech-industrial-data-historian/

From the Article: "Cisco Talos researchers found two high-severity vulnerabilities in WellinTech's KingHistorian industrial data historian software."

CISA Expands Cybersecurity Committee, Updates Baseline Security Goals

Source: https://www.securityweek.com/cisa-adds-experts-to-cybersecurity-committee-updates-baseline-security-goals/

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: "CISA announces adding more experts to its Cybersecurity Advisory Committee and updating the Cybersecurity Performance Goals."

Malware Trends: What's Old Is Still New

Source: https://www.securityweek.com/malware-trends-whats-old-is-still-new/

From the Article: "Many of the most successful cybercriminals are shrewd; they want good ROI, but they don't want to have to reinvent the wheel to get it."

Ransomware Gang Publishes Data Allegedly Stolen From Maritime Firm Royal Dirkzwager

Source: https://www.securityweek.com/ransomware-gang-publishes-data-allegedly-stolen-from-maritime-firm-royal-dirkzwager/

From the Article: "The Play ransomware gang has published data stolen from Dutch maritime services company Royal Dirkzwager."

Exploitation of 55 Zero-Day Vulnerabilities Came to Light in 2022: Mandiant

Source: https://www.securityweek.com/exploitation-of-55-zero-day-vulnerabilities-came-to-light-in-2022-mandiant/

From the Article: "Mandiant has conducted an analysis of the zero-day vulnerabilities disclosed in 2022 and over a dozen were linked to cyberespionage groups."

Malicious NuGet Packages Used to Target .NET Developers

Source: https://www.securityweek.com/malicious-nuget-packages-used-to-target-net-developers/

From the Article: "Software developers have been targeted in a new attack via malicious packages in the NuGet repository."

Link back to Table of Contents

Google Pixel Vulnerability Allows Recovery of Cropped Screenshots

Source: https://www.securityweek.com/google-pixel-vulnerability-allows-the-recovery-of-cropped-screenshots/

From the Article: "A vulnerability in Google Pixel phones allows for the recovery of an original, unedited screenshot from the cropped version."

Organizations Notified of Remotely Exploitable Vulnerabilities in Aveva HMI, SCADA Products

Source: https://www.securityweek.com/organizations-notified-of-remotely-exploitable-vulnerabilities-in-aveva-hmi-scada-products/

From the Article: "Industrial organizations using HMI and SCADA products from Aveva have been informed about potentially serious vulnerabilities."

Millions Stolen in Hack at Cryptocurrency ATM Manufacturer General Bytes

Source: https://www.securityweek.com/millions-stolen-in-hack-at-cryptocurrency-atm-manufacturer-general-bytes/

From the Article: "Cryptocurrency ATM maker General Bytes discloses a security incident resulting in the theft of millions of dollars' worth of crypto-coins."

Session Cookies, Keychains, SSH Keys and More | 7 Kinds of Data Malware Steals from macOS Users

Source: https://www.sentinelone.com/blog/session-cookies-keychains-ssh-keys-and-more-7-kinds-of-data-malware-steals-from-macos-users/

From the Article: "The scourge of ransomware attacks that has plagued Windows endpoints over the past half decade or so has, thankfully, not been replicated on Mac devices. With a few unsuccessful exceptions, the notion of locking a Mac device and holding its owner to ransom in return for access to the machine and its data has not yet proven an attractive proposition for attackers."

Link back to Table of Contents

Typo ransomware

Source: https://www.2-spyware.com/remove-typo-ransomware.html

From the Article: "Typo ransomware is a dangerous threat that may result in complete data loss Typo ransomware is a type of malware that encrypts all personal files on a computer, rendering them inaccessible until a special decryption key is used."

CommonMagic APT uses new malware to target organizations in Russo-Ukrainian conflict zone

Source: https://www.2-spyware.com/commonmagic-apt-uses-new-malware-to-target-organizations-in-russo-ukrainian-conflict-zone

From the Article: "Most likely delivered via spear phishing attacks Kaspersky[1] has identified an advanced persistent threat (APT) campaign called CommonMagic that targets organizations in the Russo-Ukrainian conflict zone. "

ExilenceTG ransomware

Source: https://www.2-spyware.com/remove-exilencetg-ransomware.html

From the Article: "ExilenceTG ransomware is a dangerous virus that locks users' personal files ExilenceTG ransomware is a file-locking virus that infiltrates the system and encrypts users' personal files."

RefreshMate adware

Source: https://www.2-spyware.com/remove-refreshmate-adware.html

From the Article: "RefreshMate is a browser extension that causes pop-up spam, redirects, and other unwanted symptoms RefreshMate is marketed as a useful plugin that can refresh all of your open tabs with a single click, but it is actually adware."

How You Can Master Supply Chain Risk

Source: https://blog.blueyonder.com/how-you-can-master-supply-chain-risk/

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: "Media outlets, as well as financial institutions like the New York Federal Reserve, are noting that supply chain pressures have eased significantly since the onset of the COVID-19 pandemic three years ago. This should have a positive impact on both general levels of inflation and the financial statements of many companies."

China's use of rhetorical adaptation in development of a global cyber order: a case study of the norm of the protection of the public core of the internet

Source: https://www.tandfonline.com/doi/full/10.1080/23738871.2023.2178946

From the Article: "How does China shape a global information order, regarding the norms and institutions that manage cyberspace? Cyber norms are the preferred tool to govern cyberspace given the rapidity of technological change. China's advances 'cyber sovereignty' (wangluo zhuquan) norms to reorient internet governance to the United Nations and specialist state-led international fora and emphasise the dominant position of the state regarding information management."

Exploring the relationship between IT development, poverty and cybercrime: an Armenia case study

Source: https://www.tandfonline.com/doi/full/10.1080/23738871.2023.2192234

From the Article: "This paper explores the relationship between IT development, regional poverty, and cybercrime, through the case of Armenia. Armenia was selected as it is a former Soviet state that has sought to promote the development of its IT sector in recent years, which has occurred within a context of widespread regional poverty. "

Tenable Cyber Watch: A Look at the U.S. National Cybersecurity Strategy, A Powerful AI Tech Gears Up for Prime Time, and more

Source: https://www.tenable.com/blog/tenable-cyber-watch-a-look-at-the-u-s-national-cybersecurity-strategy-a-powerful-ai-tech-gears

From the Article: "This week's edition of the Tenable Cyber Watch unpacks the White House's National Cybersecurity Strategy and explores how artificial intelligence will help cyber teams with complex 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.

Dole attack compromised employee data. New Zealand DIA CEO calls for Kiwis to protect their data. Surviving the aCropalypse.

Source: https://thecyberwire.com/podcasts/privacy-briefing/792/notes

From the Article: "Dole attack compromised employee data. New Zealand DIA CEO calls for Kiwis to protect their data. Surviving the aCropalypse."

Ransomware attack against Hitachi. Are extreme extortion tactics good news? Google Pixel flaw reveals edited image data. Cl0p's approach to its targets.

Source: https://thecyberwire.com/podcasts/privacy-briefing/791/notes

From the Article: "Hitachi Energy says zero-day bug allowed for ransomware attack. Could ransomware attackers' extreme tactics be good news? Google Pixel flaw reveals edited image data. Cl0p's approach to its targets."

Trigona ransomware. FakeCalls mobile malware targets South Korea. BlackSnake in the RaaS criminal market.

Source: https://thecyberwire.com/newsletters/research-briefing/5/12

From the Article: "Trigona ransomware. FakeCalls mobile malware targets South Korea. BlackSnake in the RaaS criminal market."

A look at resilience: companies' ability to fight off cyberattacks.

Source: https://thecyberwire.com/stories/7efb10a9e7a0498cb409e1addc0f0722/a-look-at-resilience-companies-ability-to-fight-off-cyberattacks

From the Article: "Cisco this morning released its Cybersecurity Readiness Index, detailing the effectiveness of cybersecurity implementations against different threat vectors."

Australian consumers hit by another data breach. NBA warns fans of data breach.

Link back to Table of Contents

Source: https://thecyberwire.com/newsletters/privacy-briefing/5/53

From the Article: "Melbourne-headquartered financial services firm Latitude Financial has taken its systems offline following a cyberattack the company sustained last week, Reuters reports. The Australian Federal Police and the Australian Cyber Security Centre (ACSC) are investigating the attack. The ABC reports that over 300,000 customers have been affected by the breach, with at least 100,000 driver's licenses stolen."

Cl0p hits Hitachi Energy. TikTok surveillance investigated. BreachForums arrest. Hacktivists, torrents in the hybrid war.

Source: https://thecyberwire.com/newsletters/daily-briefing/12/53

From the Article: "Cl0p ransomware at Hitachi Energy. US Department of Justice investigates ByteDance in alleged surveillance of journalists. Pompompurin arrested for alleged role in BreachForums."

2023 Cybersecurity Maturity Report Reveals Organizational Unpreparedness for Cyberattacks

Source: https://thehackernews.com/2023/03/2023-cybersecurity-maturity-report.html

From the Article: "In 2022 alone, global cyberattacks increased by 38%, resulting in substantial business loss, including financial and reputational damage. Meanwhile, corporate security budgets have risen significantly because of the growing sophistication of attacks and the number of cybersecurity solutions introduced into the market. "

Operation Soft Cell: Chinese Hackers Breach Middle East Telecom Providers

Source: https://thehackernews.com/2023/03/operation-soft-cell-chinese-hackers.html

From the Article: "Telecommunication providers in the Middle East are the subject of new cyber attacks that commenced in the first quarter of 2023."

ScarCruft's Evolving Arsenal: Researchers Reveal New Malware Distribution 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.

Source: https://thehackernews.com/2023/03/scarcrufts-evolving-arsenal-researchers.html

From the Article: "The North Korean advanced persistent threat (APT) actor dubbed ScarCruft is using weaponized Microsoft Compiled HTML Help (CHM) files to download additional malware onto targeted machines."

Preventing Insider Threats in Your Active Directory

Source: https://thehackernews.com/2023/03/preventing-insider-threats-in-your.html

From the Article: "Active Directory (AD) is a powerful authentication and directory service used by organizations worldwide. With this ubiquity and power comes the potential for abuse."

Rogue NuGet Packages Infect .NET Developers with Crypto-Stealing Malware

Source: https://thehackernews.com/2023/03/rogue-nuget-packages-infect-net.html

From the Article: "The NuGet repository is the target of a new "sophisticated and highly-malicious attack" aiming to infect .NET developer systems with cryptocurrency stealer malware."

New 'Bad Magic' Cyber Threat Disrupts Ukraine's Key Sectors Amid War

Source: https://thehackernews.com/2023/03/new-bad-magic-cyber-threat-disrupt.html

From the Article: "Amid the ongoing war between Russia and Ukraine, government, agriculture, and transportation organizations located in Donetsk, Lugansk, and Crimea have been attacked as part of an active campaign that drops a previously unseen, modular framework dubbed CommonMagic."

New DotRunpeX Malware Delivers Multiple Malware Families via Malicious Ads

Source: https://thehackernews.com/2023/03/new-dotrunpex-malware-delivers-multiple.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: "A new piece of malware dubbed dotRunpeX is being used to distribute numerous known malware families such as Agent Tesla, Ave Maria, BitRAT, FormBook, LokiBot, NetWire, Raccoon Stealer, RedLine Stealer, Remcos, Rhadamanthys, and Vidar."

New Cyber Platform Lab 1 Decodes Dark Web Data to Uncover Hidden Supply Chain Breaches

Source: https://thehackernews.com/2023/03/new-cyber-platform-lab-1-decodes-dark.html

From the Article: "2022 was the year when inflation hit world economies, except in one corner of the global marketplace – stolen data. Ransomware payments fell by over 40% in 2022 compared to 2021. More organisations chose not to pay ransom demands, according to findings by blockchain firm Chainalysis."

Researchers Shed Light on CatB Ransomware's Evasion Techniques

Source: https://thehackernews.com/2023/03/researchers-shed-light-on-catb.html

From the Article: "The threat actors behind the CatB ransomware operation have been observed using a technique called DLL search order hijacking to evade detection and launch the payload."

A New Security Category Addresses Web-borne Threats

Source: https://thehackernews.com/2023/03/a-new-security-category-addresses-web.html

From the Article: "In the modern corporate IT environment, which relies on cloud connectivity, global connections and large volumes of data, the browser is now the most important work interface. The browser connects employees to managed resources, devices to the web, and the on-prem environment to the cloud one."

New Cryptojacking Operation Targeting Kubernetes Clusters for Dero Mining

Source: https://thehackernews.com/2023/03/new-cryptojacking-operation-targeting.html

Link back to Table of Contents

From the Article: "Cybersecurity researchers have discovered the first-ever illicit cryptocurrency mining campaign used to mint Dero since the start of February 2023."

Researchers Uncover Over a Dozen Security Flaws in Akuvox E11 Smart Intercom

Source: https://thehackernews.com/2023/03/researchers-uncover-over-dozen-security.html

From the Article: "More than a dozen security flaws have been disclosed in E11, a smart intercom product made by Chinese company Akuvox."

International Law Enforcement Takes Down Infamous NetWire Cross-Platform RAT

Source: https://thehackernews.com/2023/03/international-law-enforcement-takes.html

From the Article: "A coordinated international law enforcement exercise has taken down the online infrastructure associated with a cross-platform remote access trojan (RAT) known as NetWire."

Xenomorph Android Banking Trojan Returns with a New and More Powerful Variant

Source: https://thehackernews.com/2023/03/xenomorph-android-banking-trojan.html

From the Article: "A new variant of the Android banking trojan named Xenomorph has surfaced in the wild, latest findings from ThreatFabric reveal."

Uncle Sam reveals it sent cyber-soldiers to Albania to hunt for Iranian threats

Source: https://www.theregister.com/2023/03/24/us_hunt_forward_albania/

From the Article: "US Cyber Command operators have confirmed they carried out an online defensive mission in Albania, in response to last year's cyber attacks against the local government."

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.

South Korea fines McDonald's for data leak from raw SMB share

Source:
https://www.theregister.com/2023/03/23/south_korea_privacy_fines_mcdonalds/

From the Article: "South Korea's Personal Information Protection Commission has fined McDonald's, British American Tobacco, and Samsung for privacy breaches."

Cisco kindly reveals proof of concept attacks for flaws in rival Netgear's kit

Source: https://www.theregister.com/2023/03/22/netgear_router_poc_exploits/

From the Article: "Public proof-of-concept exploits have landed for bugs in Netgear Orbi routers – including one critical command execution vulnerability."

Australian FinTech takes itself offline to deal with cyber incident that caused data leak

Source: https://www.theregister.com/2023/03/21/latitude_financial_cyber_attack_leak/

From the Article: "Latitude Financial has blamed a supplier for leaking creds that caused vast PII leak Australian outfit Latitude Financial has taken itself offline, and even stopped serving customers, while it tries to clean up an attack on its systems."

UK refreshes national security plan to stop more of China's secret-stealing cyber-tricks

Source: https://www.theregister.com/2023/03/14/uk_integrated_review_refresh/

From the Article: "Britain's domestic intelligence service MI5 will oversee a new agency tasked with helping organizations combat Chinese cyber-spies and other threats."

Nordic countries set shared cyber plan. Remedying US cybersecurity regulatory issues. TikTok preps for congressional hearing.

Source: https://thecyberwire.com/newsletters/policy-briefing/5/55

From the Article: "Nordic countries establish a shared cybersecurity plan. Remedying the US's cybersecurity regulatory issues. TikTok prepares for congressional hearing."

Link back to Table of Contents

Ransomware attack against Hitachi. Are extreme extortion tactics good news? Google Pixel flaw reveals edited image data. Cl0p's approach to its targets.

Source: https://thecyberwire.com/newsletters/privacy-briefing/5/55

From the Article: "Hitachi Energy says zero-day bug allowed for ransomware attack. Could ransomware attackers' extreme tactics be good news? Google Pixel flaw reveals edited image data. Cl0p's approach to its targets."

Trigona ransomware. FakeCalls mobile malware targets South Korea. BlackSnake in the RaaS criminal market.

Source: https://thecyberwire.com/newsletters/research-briefing/5/12

From the Article: "Trigona ransomware. FakeCalls mobile malware targets South Korea. BlackSnake in the RaaS criminal market."

A look at resilience: companies' ability to fight off cyberattacks.

Source: https://thecyberwire.com/stories/7efb10a9e7a0498cb409e1addc0f0722/a-look-at-resilience-companies-ability-to-fight-off-cyberattacks

From the Article: "Cisco this morning released its Cybersecurity Readiness Index, detailing the effectiveness of cybersecurity implementations against different threat vectors."

Cl0p ransomware at Hitachi Energy. Alleged TikTok surveillance of journalists. Hacktivist auxiliary hits Indian healthcare records. Cyberattack on Latitude: update. BreachForums arrest.

Source: https://thecyberwire.com/podcasts/daily-podcast/1783/notes

From the Article: "Cl0p ransomware hits Hitachi Energy. The US Department of Justice investigates ByteDance in alleged surveillance of journalists. A Hacktivist auxiliary hits Indian healthcare records."

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.

Operation Soft Cell: Chinese Hackers Breach Middle East Telecom Providers

Source: https://thehackernews.com/2023/03/operation-soft-cell-chinese-hackers.html

From the Article: "Telecommunication providers in the Middle East are the subject of new cyber attacks that commenced in the first quarter of 2023."

ScarCruft's Evolving Arsenal: Researchers Reveal New Malware Distribution Techniques

Source: https://thehackernews.com/2023/03/scarcrufts-evolving-arsenal-researchers.html

From the Article: "The North Korean advanced persistent threat (APT) actor dubbed ScarCruft is using weaponized Microsoft Compiled HTML Help (CHM) files to download additional malware onto targeted machines."

Preventing Insider Threats in Your Active Directory

Source: https://thehackernews.com/2023/03/preventing-insider-threats-in-your.html

From the Article: "Active Directory (AD) is a powerful authentication and directory service used by organizations worldwide. With this ubiquity and power comes the potential for abuse."

Rogue NuGet Packages Infect .NET Developers with Crypto-Stealing Malware

Source: https://thehackernews.com/2023/03/rogue-nuget-packages-infect-net.html

From the Article: "The NuGet repository is the target of a new "sophisticated and highly-malicious attack" aiming to infect .NET developer systems with cryptocurrency stealer malware."

New 'Bad Magic' Cyber Threat Disrupts Ukraine's Key Sectors Amid War

Source: https://thehackernews.com/2023/03/new-bad-magic-cyber-threat-disrupt.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: "Amid the ongoing war between Russia and Ukraine, government, agriculture, and transportation organizations located in Donetsk, Lugansk, and Crimea have been attacked as part of an active campaign that drops a previously unseen, modular framework dubbed CommonMagic."

New DotRunpeX Malware Delivers Multiple Malware Families via Malicious Ads

Source: https://thehackernews.com/2023/03/new-dotrunpex-malware-delivers-multiple.html

From the Article: "A new piece of malware dubbed dotRunpeX is being used to distribute numerous known malware families such as Agent Tesla, Ave Maria, BitRAT, FormBook, LokiBot, NetWire, Raccoon Stealer, RedLine Stealer, Remcos, Rhadamanthys, and Vidar."

New Cyber Platform Lab 1 Decodes Dark Web Data to Uncover Hidden Supply Chain Breaches

Source: https://thehackernews.com/2023/03/new-cyber-platform-lab-1-decodes-dark.html

From the Article: "2022 was the year when inflation hit world economies, except in one corner of the global marketplace – stolen data. Ransomware payments fell by over 40% in 2022 compared to 2021. More organisations chose not to pay ransom demands, according to findings by blockchain firm Chainalysis."

Researchers Shed Light on CatB Ransomware's Evasion Techniques

Source: https://thehackernews.com/2023/03/researchers-shed-light-on-catb.html

From the Article: "The threat actors behind the CatB ransomware operation have been observed using a technique called DLL search order hijacking to evade detection and launch the payload."

A New Security Category Addresses Web-borne Threats

Source: https://thehackernews.com/2023/03/a-new-security-category-addresses-

web.html

From the Article: "In the modern corporate IT environment, which relies on cloud connectivity, global connections and large volumes of data, the browser is now the most important work interface. The browser connects employees to managed resources, devices to the web, and the on-prem environment to the cloud one."

New Cryptojacking Operation Targeting Kubernetes Clusters for Dero Mining

Source: https://thehackernews.com/2023/03/new-cryptojacking-operation-targeting.html

From the Article: "Cybersecurity researchers have discovered the first-ever illicit cryptocurrency mining campaign used to mint Dero since the start of February 2023."

Researchers Uncover Over a Dozen Security Flaws in Akuvox E11 Smart Intercom

Source: https://thehackernews.com/2023/03/researchers-uncover-over-dozen-security.html

From the Article: "More than a dozen security flaws have been disclosed in E11, a smart intercom product made by Chinese company Akuvox."

Xenomorph Android Banking Trojan Returns with a New and More Powerful Variant

Source: https://thehackernews.com/2023/03/xenomorph-android-banking-trojan.html

From the Article: "A new variant of the Android banking trojan named Xenomorph has surfaced in the wild, latest findings from ThreatFabric reveal."

Uncle Sam reveals it sent cyber-soldiers to Albania to hunt for Iranian threats

Source: https://www.theregister.com/2023/03/24/us_hunt_forward_albania/

From the Article: "US Cyber Command operators have confirmed they carried out an online defensive mission in Albania, in response to last year's cyber attacks against the local government."

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.

South Korea fines McDonald's for data leak from raw SMB share

Source: https://www.theregister.com/2023/03/23/south_korea_privacy_fines_mcdonalds/

From the Article: "South Korea's Personal Information Protection Commission has fined McDonald's, British American Tobacco, and Samsung for privacy breaches."

Cisco kindly reveals proof of concept attacks for flaws in rival Netgear's kit

Source: https://www.theregister.com/2023/03/22/netgear_router_poc_exploits/

From the Article: "Public proof-of-concept exploits have landed for bugs in Netgear Orbi routers – including one critical command execution vulnerability."

Australian FinTech takes itself offline to deal with cyber incident that caused data leak

Source: https://www.theregister.com/2023/03/21/latitude_financial_cyber_attack_leak/

From the Article: "Latitude Financial has blamed a supplier for leaking creds that caused vast PII leak Australian outfit Latitude Financial has taken itself offline, and even stopped serving customers, while it tries to clean up an attack on its systems."

UK refreshes national security plan to stop more of China's secret-stealing cyber-tricks

Source: https://www.theregister.com/2023/03/14/uk_integrated_review_refresh/

From the Article: "Britain's domestic intelligence service MI5 will oversee a new agency tasked with helping organizations combat Chinese cyber-spies and other threats."

Gordon Moore, Intel Co-Founder, Dies at 94

Source: https://www.intel.com/content/www/us/en/newsroom/news/gordon-moore-obituary.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: "Moore, who set the course for the future of the semiconductor industry, devoted his later years to philanthropy."

Deutsche bank stock drops fears banking crisis will get worse

Source: https://www.fastcompany.com/90871185/deutsche-bank-stock-drops-fears-banking-crisis-will-get-worse

From the Article: "Deutsche Bank shares were down 8.8% in late-afternoon trading on the German stock exchange after falling as much as 14%."

Bulgarian Woman Charged For Role In Multi-Billion-Dollar Cryptocurrency Pyramid Scheme "OneCoin" And Extradited From Bulgaria To The United States

Source: https://www.justice.gov/usao-sdny/pr/bulgarian-woman-charged-role-multi-billion-dollar-cryptocurrency-pyramid-scheme-onecoin

From the Article: "Dilkinska was Head of Legal and Compliance for Fraudulent Cryptocurrency Marketed and Sold to Millions of Victims Around the World, Resulting in Billions of Dollars in Losses"

Nvidia works tsmc asml and synopsis software speed chipmaking

Source: https://www.fierceelectronics.com/electronics/nvidia-works-tsmc-asml-and-synopsis-software-speed-chipmaking

From the Article: "Nvidia announced a cuLitho software library for computational lithography at GTC 2023 that will be deployed by TSMC for its fabrication work starting in June."

China unveils indigenous chiplet interface to reach self-reliance amid US containment

Source: https://www.digitimes.com/news/a20230323VL203/china-chip-war-chiplet.html

From the Article: "As China is getting isolated as a result of the US technological containment, China has come up with an indigenous interconnected interface for chiplet

as Moore's law seems to approach its limits."

Potential Applied Materials factory hits snag as Hutto returns $200K for land option

Source: https://www.bizjournals.com/austin/news/2023/03/08/applied-materials-hutto-acropolis-williamson-co.html

From the Article: "But project not completely dead, city official says"

TSMC founder: "In the chip sector, globalization is dead."

Source: https://english.cw.com.tw/article/article.action?id=3396

From the Article: "Morris Chang, the founder of TSMC, shared his support for US efforts to slow China's progress in chip production at a recent semiconductor forum hosted by CommonWealth magazine. However, Chang also warned that "globalization, at least in the chips sector, is dead," and raised concerns that US onshoring policies could lead to the price of chips increasing."

TSMC to see 5/4nm chip sales produce additional NT$100 billion in 2023

Source: https://www.digitimes.com/news/a20230322PD211/4nm-chips+components-ic-manufacturing-revenue-tsmc.html

From the Article: "TSMC is expected to see 5nm and 4nm chip sales generate an additional NT$100 billion in 2023, despite a roughly flat revenue growth this year, according to industry sources."

Taiwan foundries see surge in orders transferred from China

Source: https://www.digitimes.com/news/a20230323PD216/china-chip-war-ic-manufacturing-smic-tsmc.html

From the Article: "The US' escalation of the chip war with China has prompted more companies to shift their orders to Taiwan-based pure-play foundries. However, contract prices provided by TSMC and other Taiwanese foundries for orders transferred from Chinese counterparts..."

Link back to Table of Contents

Vishay is building the next chip factory in Germany

Source: https://www.faz.net/aktuell/wirtschaft/unternehmen/naechste-chipfabrik-in-deutschland-18760304.html

From the Article: "The American semiconductor group is building a new one next to its old plant in Itzehoe. It costs him $350 million."

ASML set for victory in competition for AI chips

Source: https://www.theregister.com/2023/03/24/asml_clear_winner_in_run/

From the Article: " It's the only game in town for extreme ultraviolet lithography, and that makes it every chip shop's new best friend"

Chip designer Arm plans to increase profits by refining its business model - SiliconANGLE

Source: https://siliconangle.com/2023/03/23/chip-designer-arm-plans-increase-profits-refining-business-model/

From the Article: "The Financial Times, which first reported the news, cited several industry executives and former Arm employees as saying that the company will begin charging device makers for its chip designs, with fees based on the value of the device sold."

Nvidia's CEO talks about trends towards ChatGPT and large language models

Source: https://www.digitimes.com/news/a20230323VL202.html

From the Article: "Nvidia CEO Jensen Huang at this year's GPU Technology Conference (GTC) discussed a variety of subjects and technological development trends, particularly those related to accelerated computing and AI. In a Q&A call hosted by Nvidia for the press..."

Link back to Table of Contents

'No line to be drawn' in tech war with China, says former Commerce Department BIS official

Source: https://www.digitimes.com/news/a20230324VL204/china-chip-war-tsmc.html

From the Article: "US-China relations hit a new low in February as Washington added six Chinese companies to its Entity List in connection with the balloon incident. To complement the export controls against the Chinese chip industry introduced by the US in October 2022,..."

Taiwan PCB makers moving production to Southeast Asia

Source: https://www.digitimes.com/news/a20230323PD214/malaysia-manufacturing-pcb-manufacturing-printed-circuit-board-southeast-asia-taiwan-thailand-vietnam.html

From the Article: "Taiwan-based printed circuit board (PCB) makers have expedited transferring manufacturing away from China, with several establishing new plants or extending current lines in Southeast Asia, particularly Thailand, Malaysia, and Vietnam."

Epi-wafer supplier IntelliEPI upbeat about industrial, military defense demand

Source: https://www.digitimes.com/news/a20230323PD212/5g-6g-defense-epi-wafer-epitaxial-wafer-gaas-gasb-intelliepi-military.html

From the Article: "Epitaxial wafer (epi wafer) supplier Intelligent Epitaxy Technology (IntelliEPI) is optimistic about demand for industrial and military defense applications, as well as demand for 5G and 6G connectivity devices."

Pegatron chairman notes the trend of 'small AI' chips amid a new wave of AI arms race

Source: https://www.digitimes.com/news/a20230324PD209/chatgpt-china-pegatron.html

From the Article: "In a discussion with the famed AI scientist Fei-Fei Li at a forum on March 23, Pegratron chairman T.H. Tung remarked that the current stage of AI development is still not mature enough to replace humans, though AI will strengthen human judgment. "

Link back to Table of Contents

L&K lands over NT$18 billion worth of orders for new UMC fab in Singapore

Source: https://www.digitimes.com/news/a20230324VL203/fab-ic-manufacturing-singapore-umc.html

From the Article: "So far in 2023, cleanroom contractor L&K Engineering has secured orders totaling NT$18.62 billion (US$613.7 million) from United Microelectronics (UMC) for the pure-play foundry's new fab in Singapore."

IC Design White Paper (5): China's semiconductor strategy and development trends

Source: https://www.digitimes.com/news/a20230317PD204/ic-design-white-paper-china-taiwan-us-china-chip-ban.html

From the Article: "China has had a long history of supporting its semiconductor development with industrial policies. The "Outline for advancing the national IC industry" announced in 2014 upgraded semiconductors from a matter of industrial policy to national development..."

Taiwan chip exports to China sputter on tensions, falling demand

Source: https://www.digitimes.com/news/a20230320VL210/china.html

From the Article: "Taiwan's exports of integrated circuit chips to China and Hong Kong fell for a fourth month in February as Washington-Beijing tensions simmer and demand for electronics continues to drop off."

Resonac enters mass production of new-gen SiC epi-wafers for EVs

Source: https://www.digitimes.com/news/a20230316PD202/chips+components-showa-denko-resonac-sic.html

From the Article: "Japan-based Resonac, formerly Showa Denko, kicked off volume production of its new-generation 6-inch SiC epi-wafers on March 1, aiming to serve the needs of EVs and other high-end applications."

IC design may serve as key for Malaysia to further enhance local semiconductor

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.

competitiveness, says DIGITIMES Research

Source: https://www.digitimes.com/news/a20230324VL205/digitimes-research-ic-manufacturing-malaysia-semiconductor.html

From the Article: "With the US-China trade war and the COVID-19 pandemic driving companies to diversify their production lines to different parts of the world to avoid risks after 2020, Malaysia has also become one of the targets for international first-tier IT companies..."

Intel's acquisition of Tower Semiconductor expected to be completed in 1H23

Source: https://www.digitimes.com/news/a20230323VL201/acquisition-ic-manufacturing-intel-tower-semiconductor.html

From the Article: "After more than 12 months, Intel said the planned acquisition of Israel-based Tower Semiconductor might be delayed again and is expected to be completed by the first half of 2023."

Taiwan wafer foundry experiences first sequential revenue decline since start of COVID-19 in 4Q22, says DIGITIMES Research

Source: https://www.digitimes.com/news/a20230323VL206/4q22-chips+components-digitimes-research-foundry-ic-manufacturing-revenue.html

From the Article: "The four leading foundries in Taiwan - Taiwan Semiconductor Manufacturing Company (TSMC), United Microelectronics (UMC), Powerchip Semiconductor Manufacturing (PSMC), and Vanguard International Semiconductor (VIS) - together generated a total of US$89.4..."

Taiwan wafer foundry industry, 4Q22

Source: https://www.digitimes.com/news/a20230323RS400.html&chid=2

From the Article: "The four leading foundries in Taiwan - Taiwan Semiconductor Manufacturing Company (TSMC), United Microelectronics (UMC), Powerchip Semiconductor Manufacturing (PSMC) and Vanguard International Semiconductor (VIS) - together generated a total of US$89.4 billion in revenues in 2022, soaring 31% from a year ago."

Link back to Table of Contents

Foreign firms competing for Taiwanese IC design talent

Source: https://www.digitimes.com/news/a20230323PD200/chips+components-east-asia-ic-design-distribution-qualcomm-taiwan.html

From the Article: "While many international semiconductor firms have recently initiated massive layoffs or workforce adjustments amid the correction in global macroeconomic conditions, talent hunting in Taiwan's IC design industry reportedly remains relatively bullish,..."

1.6 Trillion Reasons to Bet on America's Future | Palm Beach Research Group

Source: https://www.palmbeachgroup.com/palm-beach-daily/1-6-trillion-reasons-to-bet-on-americas-future/

From the Article: "Last month, we told you this trend will unleash an estimated $1.6 trillion in the U.S. economy. That's based on four federal laws enacted over the past two years. They are: The Investments and Infrastructure Act. This allocates $1.2 trillion to build U.S. infrastructure for a new generation of industrial facilities over the next several years. CHIPS and Science Act. This $52.7 billion bill is hyper-focused on ensuring America reclaims its lead in semiconductor chip design. Inflation Reduction Act."

DOE Releases New Reports on Pathways to Commercial Liftoff to Accelerate Clean Energy Technologies

Source: https://www.energy.gov/articles/doe-releases-new-reports-pathways-commercial-liftoff-accelerate-clean-energy-technologies

From the Article: "New Department-wide Initiative Will Drive Public and Private Sector Engagement Critical to Effective Clean Energy Industrial Strategy"

Cyber Sessions: Chasing talent

Source: https://pbn.com/cyber-sessions-chasing-talent/

From the Article: "Even as tech companies are making headlines for laying off portions

of their workforce, cybersecurity workers continue to be in high demand. While not completely immune from these major rounds of layoffs, cybersecurity is considered to be one of the most resilient areas for investment, even in this prudent economic atmosphere."

China frees top chip investor to bolster semiconductor efforts

Source: https://www.ft.com/content/ffb81a37-5239-4d5b-80b6-2b318084b460

From the Article: "Head of Hua Capital released from detention as Beijing seeks expert help to navigate tough western sanctions"

Free Cybersecurity Services and Tools | CISA

Source: https://www.cisa.gov/resources-tools/resources/free-cybersecurity-services-and-tools

From the Article: "As part of our continuing mission to reduce cybersecurity risk across U.S. critical infrastructure partners and state, local, tribal, and territorial governments, CISA has compiled a list of free cybersecurity tools and services to help organizations further advance their security capabilities."

US Officials Urged to Examine Chinese Risk to Electric Grid

Source: https://www.bankinfosecurity.com/us-officials-urged-to-examine-chinese-risk-to-electric-grid-a-21508

From the Article: "Utility Vendors Have Cut Back on Buying Chinese Transformers Due to Security Risks"

With U.S. trip, Taiwan leader may be aiming to temper China's ire, ex-diplomat says

Source: https://www.japantimes.co.jp/news/2023/03/26/asia-pacific/politics-diplomacy-asia-pacific/taiwan-ait-william-stanton-interview/

From the Article: "TAIPEI – Taiwanese President Tsai Ing-wen's reported plan to meet U.S. House Speaker Kevin McCarthy during a trip to the United States instead of back

home appears to be Taipei's way of trying to avoid increased tensions with China after a controversial trip to the island by McCarthy's predecessor, Nancy Pelosi, last year, according to a former U.S. diplomat."

What US spies think about China - Taipei Times

Source: https://www.taipeitimes.com/News/editorials/archives/2023/03/26/2003796735

From the Article: "The US intelligence community's annual threat assessment for this year certainly cannot be faulted for having a narrow focus or Pollyanna perspective. From a rising China, Russian aggression and Iran's nuclear ambitions, to climate change, future pandemics and the growing reach of international organized crime, US intelligence analysis is as comprehensive as it is worrying."

Biden, Trudeau call for peace in Strait - Taipei Times

Source: https://www.taipeitimes.com/News/front/archives/2023/03/26/2003796741

From the Article: "US President Joe Biden and Canadian Prime Minister Justin Trudeau on Friday issued a joint statement reiterating the importance of maintaining peace and stability in the Taiwan Strait, as they encouraged Beijing and Taipei to resolve issues peacefully."

Talent shortage top issue for chipmaking industry - Taipei Times

Source: https://www.taipeitimes.com/News/biz/archives/2023/03/24/2003796617

From the Article: "Advancing forward-looking semiconductor research and nurturing talent require long-term joint efforts by the industry, government and academia, Taiwan Semiconductor Manufacturing Co (TSMC, 台積電) corporate research director Marvin Chang (張孟凡) said."

US official announces chip delegation to visit Taiwan - Taipei Times

Source: https://www.taipeitimes.com/News/taiwan/archives/2023/03/23/2003796587

From the Article: "The US is to send officials in charge of chip development to Taiwan,

Japan and South Korea to promote cooperation in the global semiconductor supply chain, the US Department of Commerce said on Tuesday."

German minister leads historic visit to Taiwan - Taipei Times

Source: https://www.taipeitimes.com/News/front/archives/2023/03/22/2003796518

From the Article: "Taiwan and Germany yesterday morning inked an agreement on scientific and technological cooperation, with the first German federal Cabinet minister to visit Taiwan in 26 years presiding over the ceremony."

New US rules not to force China fab closures: Seoul - Taipei Times

Source: https://www.taipeitimes.com/News/biz/archives/2023/03/23/2003796560

From the Article: "The US Department of Commerce on Tuesday proposed limits for recipients of US chip manufacturing and research funding, including limits on investing in expansion in countries such as China and Russia. The world's largest and second-largest memorychip makers, Samsung Electronics Co and SK Hynix Inc, have chip production facilities in China."

Chip war and censorship hobble Chinese tech giants in chatbot race - Taipei Times

Source: https://www.taipeitimes.com/News/feat/archives/2023/03/23/2003796573

From the Article: "Search giant Baidu's lacklustre unveiling of its chatbot exposed gaps in China's race to rival ChatGPT, as censorship and a US squeeze on chip imports have hamstrung the country's artificial intelligence ambitions."

Taiwan tops SEMI's spending forecast - Taipei Times

Source: https://www.taipeitimes.com/News/biz/archives/2023/03/23/2003796554

From the Article: "SEMICONDUCTOR EQUIPMENT: The international trade group said the sector would recover from a slump, with spending expected to rise 4.2 percent to US$24.9 billion"

Link back to Table of Contents

EDITORIAL: TSMC concerns worth listening to - Taipei Times

Source: https://www.taipeitimes.com/News/editorials/archives/2023/03/21/2003796444

From the Article: "Taiwan Semiconductor Manufacturing Co (TSMC) founder Morris Chang (張忠謀) has repeatedly voiced concern over the weakening cost competitiveness of its US fabs and challenged the US' "on-shore" policy of building domestic semiconductor capacity. Yet not once has the government said anything, even though the economy is highly dependent on the chip industry."

The Race Toward Mixed-Foundry Chiplets

Source: https://semiengineering.com/the-race-toward-mixed-foundry-chiplets/

From the Article: "The challenges of assembling chiplets from different foundries are just beginning to emerge."

Week In Review: Manufacturing, Test

Source: https://semiengineering.com/week-in-review-manufacturing-test-222/

From the Article: "Toshiba favors takeover bid; ASIC publishes National Advanced Packaging Manufacturing Program whitepaper; SEMI's World Fab Forecast; Nova opens new facility; Samsung's first UWB chipset, NVIDIA tweaks chip for China and announces Quantum processor."

Week In Review: Auto, Security, Pervasive Computing

Source: https://semiengineering.com/week-in-review-auto-security-pervasive-computing-160/

From the Article: "EV profit eludes Ford for now; Infineon, Delta MOU for EV tech; Hyundai's car-charging robot."

Week In Review: Design, Low Power

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://semiengineering.com/week-in-review-design-low-power-239/

From the Article: "Renesas' new acquisition; NVIDIA partnerships; EDA's big changes; battery drain tool; complexity of 3D designs; chiplets integration & mini-consortia; China build out; thermal management; quantum computer deployment."

True 3D Is Much Tougher Than 2.5D

Source: https://semiengineering.com/true-3d-is-much-tougher-than-2-5d/

From the Article: "While terms often are used interchangeably, they are very different technologies with different challenges."

Managing EDA's Rapid Growth Expectations

Source: https://semiengineering.com/managing-edas-rapid-growth-expectations/

From the Article: "EDA is growing quickly, fueled by many changes in the chip industry. But can it keep up and continue to satisfy the needs of all its customers?"

DoD decades behind private sector in recruiting talent for civilian jobs, study finds | Federal News Network

Source: https://federalnewsnetwork.com/defense-news/2023/03/dod-decades-behind-private-sector-in-recruiting-talent-for-civilian-jobs-study-finds/

From the Article: "An influential Defense advisory board has a harsh critique of the Defense Department's strategies for recruiting talent into its civilian ranks: There isn't much of a strategy at all. The new Defense Business Board (DBB) study also found the Pentagon, as a general matter, doesn't have a discernable talent pipeline for civilians, and that little effort has been spent to market DoD as an attractive civilian employer."

Inaudible ultrasound attack can stealthily control your phone, smart speaker

Source: https://www.bleepingcomputer.com/news/security/inaudible-ultrasound-attack-can-stealthily-control-your-phone-smart-speaker/

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: "American university researchers have developed a novel attack called "Near-Ultrasound Inaudible Trojan" (NUIT) that can launch silent attacks against devices powered by voice assistants, like smartphones, smart speakers, and other IoTs."

Supply Chain Weekly Wrap-Up 03/17/2023-03/23/2023

Source: https://www.allthingssupplychain.com/supply-chain-weekly-wrap-up-03-17-2023-03-23-2023/

From the Article: "IBM and Canada to Unveil Chips Pact Canada and International Business Machines (IBM), look to seal an agreement to strengthen semiconductor cooperation on today. "

Threat Roundup for March 17 to March 24

Source: https://blog.talosintelligence.com/threat-roundup-0317-0324/

From the Article: "Today, Talos is publishing a glimpse into the most prevalent threats we've observed between March 17 and March 24. As with previous roundups, this post isn't meant to be an in-depth analysis."

UK parliament follows government by banning TikTok over cybersecurity concerns

Source: https://www.csoonline.com/article/3691615/uk-parliament-follows-government-by-banning-tiktok-over-cybersecurity-concerns.html

From the Article: "The commissions of the House of Commons and House of Lords have followed the UK government by banning social media app TikTok over cybersecurity concerns. A parliament spokesman said that TikTok “will be blocked from all parliamentary devices and the wider parliamentary network,” a move that TikTok has described as “misguided” and “based on fundamental misconceptions” about the company."

Weekly Cyber Threat Report, March 20 – March 24, 2023

Source: https://cyberintelmag.com/threat-intelligence/weekly-cyber-threat-report-march-

20-march-24-2023/

From the Article: "This week's good news includes CISA launching a prototype program for identifying exploitable ransomware vulnerabilities, highly severe flaws being addressed in the Chrome 111 update, the UK government announcing a plan to safeguard the NHS against cyberattacks, high-severity IOS software weaknesses being addressed by Cisco, and much more."

Latest Android Malware Found Targeting Customers of 450 Financial Institutions Globally

Source: https://cyberintelmag.com/malware-viruses/latest-android-malware-found-targeting-customers-of-450-financial-institutions-globally/

From the Article: "Customers of 450 banks and cryptocurrency services throughout the world are being targeted by a threat actor using a harmful Android Trojan that has many capabilities for taking control of online accounts and potentially draining cash from them."

PoC Exploits For Netgear Orbi Router Weaknesses Revealed

Source: https://cyberintelmag.com/cloud-security/poc-exploits-for-netgear-orbi-router-weaknesses-revealed/

From the Article: "There have been disclosed proof-of-concept exploits for bugs in the Orbi 750 series router and extender satellites from Netgear, one of which is a critical severity remote command execution bug. "

Stealthy hacks show advancements in China's cyberespionage operations, researchers say

Source: https://cyberscoop.com/china-cyberespionage-middle-east-telecoms/

From the Article: "A string of recently discovered digital intrusions appears to indicate that hackers linked to China are increasingly savvy when it comes to evading detection once they infiltrate a victim's network."

Link back to Table of Contents

Schools' Files Leak Online Days After Ransomware Deadline

Source: https://www.cysecurity.news/2023/03/schools-files-leak-online-days-after.html

From the Article: "Many documents purported to have been stolen from Minneapolis Public Schools, and have now been posted online. In the days following the announcement of the breach, a cyber gang claimed that the district did not meet its deadline to pay a ransom demand of $1 million. "

A Major Flaw in the AI Testing Framework MLflow can Compromise the Server and Data

Source: https://www.cysecurity.news/2023/03/a-major-flaw-in-ai-testing-framework.html

From the Article: "MLflow, an open-source framework used by many organizations to manage and record machine-learning tests, has been patched for a critical vulnerability that could enable attackers to extract sensitive information from servers such as SSH keys and AWS credentials."

How to Shield Yourself From Malicious Websites

Source: https://www.cysecurity.news/2023/03/how-to-shield-yourself-from-malicious.html

From the Article: "The sense of wondering if you've just infected your phone or computer with a virus is familiar if you've ever clicked on a link someone sent you, say in an email or a direct message, only to be sent to a website that seemed really suspect."

Data Breach: Data of 168 Million Citizens Stolen and Sold, 7 Suspects Arrests

Source: https://www.cysecurity.news/2023/03/data-breach-data-of-168-million.html

From the Article: "A new case of a massive data breach that would have had consequences over the national security has recently been exposed by Cyberabad Police."

To Safeguard Children from Exploitation, Parents Should Reconsider Approach to Online

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.

Behaviour

Source: https://www.cysecurity.news/2023/03/to-safeguard-children-from-exploitation.html

From the Article: "Raising children in the digital age is becoming particularly complex. Many young people are growingly reliant on screens for social interaction. They experiment with new media sharing platforms such as TikTok, Snapchat, and BeReal, but without necessarily considering long-term consequences. "

A Privacy Flaw in Windows 11's Snipping Tool Exposes Cropped Image Content

Source: https://www.cysecurity.news/2023/03/a-privacy-flaw-in-windows-11s-snipping.html

From the Article: "A serious privacy vulnerability known as 'acropalypse' has also been discovered in the Windows Snipping Tool, enabling people to partially restore content that was photoshopped out of an image. "

GitHub's Private RSA SSH Key Mistakenly Exposed in Public Repository

Source: https://www.darkreading.com/application-security/github-private-rsa-ssh-key-mistakenly-exposed-public-repository

From the Article: "GitHub hastens to replace its RSA SSH host key after an exposure mishap threatens users with man-in-the-middle attacks and organization impersonation."

Zoom Zoom: 'Dark Power' Ransomware Extorts 10 Targets in Less Than a Month

Source: https://www.darkreading.com/vulnerabilities-threats/dark-power-ransomware-extorts-10-targets-less-than-a-month

From the Article: "A new threat actor is racking up victims and showing unusual agility. Part of its success could spring from the use of the Nim programming language."

Open Source Vulnerabilities Still Pose a Big Challenge for Security Teams

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/application-security/open-source-vulnerabilities-still-pose-a-big-challenge-for-security-teams

From the Article: "Open source software continues to pose a challenge for companies. With the proper security practices, you can reduce your open source risk and manage it."

Epidemic of Insecure Storage, Backup Devices Is a Windfall for Cybercriminals

Source: https://www.darkreading.com/risk/epidemic-insecure-storage-backup-devices-cybercriminals

From the Article: "Enterprise storage devices have 14 security weaknesses on average, putting them at risk of compromise by cyberattackers and especially ransomware attacks."

Kaspersky Survey Finds One in Three Users Have Experienced CryptoTheft

Source: https://www.darkreading.com/endpoint/kaspersky-survey-finds-one-in-three-users-have-experienced-cryptotheft

From the Article: "Kaspersky has released new survey results showing that one third of crypto owners in the U.S. have experienced theft of their currency or other assets, at an average cost of $97,583. This, and other findings, are part of a new report, "Crypto Threats 2023," based on a survey of 2,000 American adults in October 2022."

Bitbucket 7.0.0 Remote Command Execution

Source: https://packetstormsecurity.com/files/171453/bitbucket700-exec.txt

From the Article: "Bitbucket version 7.0.0 suffers from a remote command execution vulnerability."

Navigating the NIS2 Directive for Enhanced Cybersecurity Resilience

Source: https://www.fortinet.com/blog/ciso-collective/navigating-nis-2-directive

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: "Learn the implications of the NIS2 Directive and gain organizational guidance to prepare for its implementation and strengthen your security posture. "

Hackers Inject Weaponized JavaScript (JS) on 51,000 Websites

Source: https://gbhackers.com/hackers-inject-weaponized-javascript/

From the Article: "Researchers from Unit 42 have been monitoring a widespread campaign of harmful JavaScript (JS) injections. The campaign aims to redirect unsuspecting victims to dangerous content, including adware and fraudulent pages."

North Korean Hackers Attack Gmail Users With Malicious Chrome Extensions

Source: https://gbhackers.com/malicious-chrome-extensions-2/

From the Article: "In a collaborative effort, the German Federal Office for the Protection of the Constitution (BfV) and the National Intelligence Service of the Republic of Korea (NIS) has released a significant cybersecurity advisory."

New Backdoor Attack Uses Russian-Ukrainian Conflict Phishing Emails

Source: https://www.hackread.com/backdoor-attack-russia-ukraine-phishing/

From the Article: "The backdoors used in this campaign are never-before-seen malware strains called CommonMagic and PowerMagic."

ChatGPT Bug Exposed Payment Details of Paid Users

Source: https://www.hackread.com/chatgpt-bug-exposed-payment-details/

From the Article: "OpenAI has apologized and reached out to affected users about the potential data breach."

TheGradCafe - 310,975 breached accounts

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

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: "In February 2023, the grad school admissions search website TheGradCafe suffered a data breach that disclosed the personal records of 310k users. The data included email addresses, names and usernames, genders, geographic locations and passwords stored as bcrypt hashes."

What Is Quishing: QR Code Phishing Explained

Source: https://heimdalsecurity.com/blog/quishing/

From the Article: "Are you aware of QR code phishing or “quishing”? This form of social engineering attack is gaining popularity among cybercriminals eager to steal your data."

Chinese Hackers Infiltrate Middle Eastern Telecom Companies

Source: https://heimdalsecurity.com/blog/chinese-hackers-infiltrate-middle-eastern-telecom-companies/

From the Article: "New cyber attacks against Middle Eastern telecommunications operators emerged in the first quarter of 2023. Based on technical overlaps, the intrusion set was identified as being the work of a Chinese cyber espionage actor associated with a long-running campaign dubbed Operation Soft Cell."

The Most Prevalent Types of Ransomware You Need to Know About

Source: https://heimdalsecurity.com/blog/most-common-types-of-ransomware/

From the Article: "Cyberthieves of today are adaptable – they are excellent at finding new ways to survive and evolve, such as creating new types of ransomware to attack our devices."

Top ways attackers are targeting your endpoints

Source: https://www.helpnetsecurity.com/2023/03/24/endpoint-vulnerability-exploitation/

From the Article: "Over the last several years, endpoints have played a crucial role in cyberattacks. While there are several steps organizations can take to help mitigate

Link back to Table of Contents

endpoint threats – such as knowing what devices are on a network (both on-premises and off-site), quarantining new or returning devices, scanning for threats and vulnerabilities, immediately applying critical patches, etc. – there is still much to be done to ensure endpoint security. "

Opti9 launches Observr ransomware detection and managed services for Veeam

Source: https://www.helpnetsecurity.com/2023/03/25/opti9-observr/

From the Article: "Opti9 Technologies has launched Observr Software-as-a-Service (SaaS) ransomware detection and standalone managed services – two new standalone service offerings that cater to organizations leveraging Veeam Software."

CISA BOD 23-01 transforms FCEB agencies, with progress led by asset detection and vulnerability enumeration

Source: https://industrialcyber.co/features/cisa-bod-23-01-transforms-fceb-agencies-with-progress-led-by-asset-detection-and-vulnerability-enumeration/

From the Article: "Heightened focus on two key operations — asset discovery and vulnerability enumeration — has taken center stage across federal civilian executive branch (FCEB) agencies, pushing them to make measurable progress across their networks."

US Senate Energy Committee addresses cybersecurity risks to critical parts of energy infrastructure

Source: https://industrialcyber.co/utilities-energy-power-water-waste/us-senate-energy-committee-addresses-cybersecurity-risks-to-critical-parts-of-energy-infrastructure/

From the Article: "The U.S. Senate Committee on Energy and Natural Resources held Thursday a full committee hearing to examine cybersecurity vulnerabilities to the nation’s energy infrastructure."

Chinese cyberespionage group Operation Soft Cell targets telecommunication providers in Middle East

Link back to Table of Contents

Source: https://industrialcyber.co/ransomware/chinese-cyberespionage-group-operation-soft-cell-targets-telecommunication-providers-in-middle-east/

From the Article: "SentinelLabs observed initial phases of attacks against telecommunication providers in the Middle East in the first quarter of this year. The team assesses that the activity represents an evolution of tooling associated with Operation Soft Cell, while it is highly likely that the threat actor is a Chinese cyberespionage group in the nexus of Gallium and APT41, the exact grouping remains unclear."

GitHub Replaces Exposed RSA SSH Key To Keep Git Operations

Source: https://informationsecuritybuzz.com/github-replaces-exposed-rsa-ssh-key-git-operations/

From the Article: "After unintentionally publishing its private SSH key, GitHub.com rotated it. The software development and version control provider took action out of “an excess of caution” after the private RSA key was briefly exposed. "

New Government Cyber Security Strategy Vital For Healthcare

Source: https://informationsecuritybuzz.com/new-government-cyber-security-strategy-healthcare/

From the Article: "The Senate Homeland Security Committee cleared legislation on March 30, 2022, aimed at enhancing the cyber readiness of the U.S. healthcare sector. The proposed “Healthcare Cybersecurity Act,” or S. 3904, calls for collaboration between the U.S."

Phishing Campaign Targets Chinese Nuclear Energy Industry

Source: https://www.intezer.com/blog/research/phishing-campaign-targets-nuclear-energy-industry/

From the Article: "Intezer has been tracking activity targeting the energy sector and noted a campaign with techniques that align with those of Bitter APT, operating in the Asia-Pacific region."

Link back to Table of Contents

Can Your Business Automate Its Ransomware Response?

Source: https://www.iotforall.com/?p=258715

From the Article: "Ransomware attacks are getting harder to stop. Luckily, automated incident response tools can help in preventing them."

Synopsys discover new vulnerability in Pluck Content Management System

Source: https://www.itsecurityguru.org/2023/03/24/synopsys-discover-new-vulnerability-in-pluck-content-management-system/

From the Article: "Pluck is a content management system (CMS) implemented in PHP designed for setting up and managing your own website. Devised with ease of use and simplicity in mind, Pluck is best suited for running a small website."

Zero-click remote hacks for Samsung, Google, and Vivo smartphones | Kaspersky official blog

Source: https://www.kaspersky.com/blog/samsung-exynos-vulnerabilities/47586/

From the Article: "This is due to the presence of 18 vulnerabilities in the Exynos baseband radio processor, which is widely used in Google, Vivo, Samsung, and many other smartphones."

New Vendor Email Compromise Attack Seeks $36 Million

Source: https://blog.knowbe4.com/36-mil-vendor-email-compromise-attack

From the Article: "The details in this thwarted VEC attack demonstrate how the use of just a few key details can both establish credibility and indicate the entire thing is a scam."

Ransomware Data Theft Extortion Goes up 40% to 70% From '21 to '22

Source: https://blog.knowbe4.com/ransomware-data-theft-extortion-goes-up

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 report from Palo Alto Networks' Unit 42 found that data theft extortion occurred in 70% of ransomware attacks in 2022, compared to 40% in 2021. The researchers examined the four most common methods of cyber extortion (encryption, data theft, harassment, and DDoS attacks) noting that threat actors often combine these tactics within a single attack campaign."

SYS01 Stealer Will Steal Your Facebook Info

Source: https://blog.morphisec.com/sys01stealer-facebook-info-stealer

From the Article: "Starting in November 2022, Morphisec has been tracking an advanced info stealer we have named "SYS01 stealer." SYS01 stealer uses similar lures and loading techniques to another information stealer recently dubbed S1deload by the Bitdefender group, but the actual payload (stealer) is different. "

Lawmakers Warn of Cyber Threat Posed by Beijing, Moscow to Energy Sector

Source: https://www.nextgov.com/cybersecurity/2023/03/lawmakers-warn-cyber-threat-posed-beijing-moscow-energy-sector/384404/

From the Article: "Enhancing collaboration and information sharing with industry partners can help mitigate threats, but concerns remain about the extent to which foreign-made equipment is embedded within the U.S. electric grid."

Acting National Cyber Director Explains New Cybersecurity Strategy to Congress

Source: https://www.nextgov.com/cybersecurity/2023/03/acting-national-cyber-director-explains-new-cybersecurity-strategy-congress/384401/

From the Article: "Acting National Cyber Director Kemba Walden highlighted some the strategy's key elements in testimony Thursday."

Vice Society claims attack on Puerto Rico Aqueduct and Sewer Authority

Source: https://securityaffairs.com/144022/hacking/puerto-rico-aqueduct-and-sewer-authority-attack.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: "Puerto Rico Aqueduct and Sewer Authority (PRASA) is investigating a cyber attack with the help of the FBI and US CISA."

New Attack Targets Online Customer Service Channels

Source: https://securityintelligence.com/articles/new-attack-targets-online-customer-service-channels/

From the Article: "Known as IceBreaker, the code is capable of stealing passwords and cookies, exfiltrating files, taking screenshots and running custom VBS scripts. While these are fairly standard functions, what sets IceBreaker apart is its infection vector. Malicious actors are leveraging the helpful nature of customer service agents to deliver their payload and drive the infection process. "

PoC Exploit Published for Just-Patched Veeam Data Backup Solution Flaw

Source: https://www.securityweek.com/poc-exploit-published-for-just-patched-veeam-data-backup-solution-flaw/

From the Article: "Proof-of-concept code to exploit a just-patched security hole in the Veeam Backup & Replication product has been published online."

CISA Gets Proactive With New Pre-Ransomware Alerts

Source: https://www.securityweek.com/cisa-gets-proactive-with-new-pre-ransomware-alerts/

From the Article: "CISA has sent notifications to more than 60 organizations as part of a new initiative to alert entities of early-stage ransomware attacks."

Cool Facts browser hijacker

Source: https://www.2-spyware.com/remove-cool-facts-browser-hijacker.html

From the Article: "Cool Facts is a useless browser extension that can cause security and privacy concerns Cool Facts is a browser hijacker that modifies the browser's default settings such as the homepage, new tab address, and search engine."

Link back to Table of Contents

Cybersecurity Snapshot: Strengthen Identity and Access Management Security with New CISA/NSA Best Practices

Source: https://www.tenable.com/blog/cybersecurity-snapshot-strengthen-identity-and-access-management-security-with-new-cisansa

From the Article: "Created by the Cybersecurity and Infrastructure Security Agency (CISA) and the National Security Agency (NSA), the document seeks to help organizations better prevent, detect and respond to IAM attacks."

Cl0p goes everywhere exploiting GoAnywhere. Latest cyber developments in the hybrid war against Ukraine. RSA Innovation Sandbox finalists announced.

Source: https://thecyberwire.com/newsletters/week-that-was/7/12

From the Article: "Cl0p goes everywhere exploiting GoAnywhere. Hacktivist auxiliary hits Indian healthcare records. Effects of cyberattack on Latitude persist. Latest updates on threat actor operations. Fresh, up-to-date trends and reports. Latest cyber developments in the hybrid war against Ukraine."

DPRK cyberespionage campaigns. Overstated hacktivist claims? Renewed Ghostwriter deception. An assessment of a cyber campaign.

Source: https://thecyberwire.com/newsletters/daily-briefing/12/56

From the Article: "DPRK threat actor Kimsuky uses Chrome extension to exfiltrate emails. DPRk's ScarCruft prospects South Korean organizations. Hacktivists' claims of attacks on OT networks are overstated."

Notes from the underworld. Cyberespionage in occupied Ukraine? Russian patriotic hacktivism in DC? Guidelines from CISA & NSA.

Source: https://thecyberwire.com/newsletters/daily-briefing/12/55

From the Article: "Baphomet backs out. Malware could detect sandbox emulations. VEC supply chain attack. Report: a new APT is active in Russian-occupied sections of

Ukraine. Someone claiming to be a Russian patriot claims responsibility for the D.C. Health Link attack."

Data breach at Ferrari. Comment on LockBit's current activities.

Source: https://thecyberwire.com/newsletters/privacy-briefing/5/54

From the Article: "Data breach at Ferrari. Comment on LockBit's current activities."

Researchers Uncover Chinese Nation State Hackers' Deceptive Attack Strategies

Source: https://thehackernews.com/2023/03/researchers-uncover-chinese-nation.html

From the Article: "A recent campaign undertaken by Earth Preta indicates that nation-state groups aligned with China are getting increasingly proficient at bypassing security solutions."

The Different Methods and Stages of Penetration Testing

Source: https://thehackernews.com/2023/03/the-different-methods-and-stages-of.html

From the Article: "The stakes could not be higher for cyber defenders. With the vast amounts of sensitive information, intellectual property, and financial data at risk, the consequences of a data breach can be devastating. "

GitHub publishes RSA SSH host keys by mistake, issues update

Source: https://www.theregister.com/2023/03/24/github_changes_its_ssh_host/

From the Article: "GitHub has updated its SSH keys after accidentally publishing the private part to the world."

Critical infrastructure gear is full of flaws, but hey, at least it's certified

Source: https://www.theregister.com/2023/03/23/critical_infrastructure_hardware_flaws/

Link back to Table of Contents

From the Article: "Devices used in critical infrastructure are riddled with vulnerabilities that can cause denial of service, allow configuration manipulation, and achieve remote code execution, according to security researchers."

The Cost of Tax Season Fraud: How Threat Actors Target Your Data and Money

Source: https://flashpoint.io/blog/the-cost-of-tax-season/

From the Article: "The IRS identified a staggering $5.7 billion in tax fraud schemes last year, over twice the amount reported in 2021. And with the large amount of personally identifiable information (PII) that is exchanged leading up to Tax Day on April 15, it's no wonder that threat actors view this time of year as high season for stealing data to exploit people's vulnerabilities for financial gain."

Tailoring Sandbox Techniques to Hidden Threats

Source: https://unit42.paloaltonetworks.com/tailoring-sandbox-techniques/

From the Article: "Techniques such as dependency emulation and analysis of encrypted network traffic can help detect malware samples that would not normally execute in a sandbox environment."

Password Hash Leakage

Source: http://windowsir.blogspot.com/2023/03/password-hash-leakage.html

From the Article: "If you've been in the security community for even a brief time, or you've taking training associated with a certification in this field, you've likely encountered the concept of password hashes. "

Subscription Required

Chinese Antigraft Watchdog Lodges Corruption Allegations Against Ex-Head of Chip Conglomerate

Source: https://www.wsj.com/articles/china-cites-chip-conglomerates-former-chief-in-

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.

corruption-probe-ed5724b0?mod=Searchresults_pos1&page=1

From the Article: "Case of Tsinghua Unigroup's ex-chairman is latest in a series of probes targeting the semiconductor industry"

Chip Makers Find Out How to Get 25% Investment Tax Credit

Source: https://www.wsj.com/articles/chip-makers-to-find-out-how-to-get-25-investment-tax-credit-ce414dd6?mod=Searchresults_pos2&page=1

From the Article: "Treasury Department proposes definitions for key terms for tax break that is estimated to cost $24 billion"

Skilled Workers Shortage Threatens Biden's Plans For U.S. Chipmaking - Tech News Briefing - WSJ Podcasts

Source: https://www.wsj.com/podcasts/tech-news-briefing/skilled-workers-shortage-threatens-bidens-plans-for-us-chipmaking/b8546879-9c5b-418e-9baa-afbda4696e12?mod=Searchresults_pos4&page=1

From the Article: "Chipmaker Micron will have to overcome a massive shortage of skilled workers in order to open its planned semiconductor-manufacturing campus in the suburbs of Syracuse, N.Y. WSJ reporter Joseph De Avila joins host Zoe Thomas to discuss how the company is dealing with the shortage and what it says about the Biden administration's goal of increasing chipmaking in the U.S."

Nvidia Is Winning AI Race, but Can't Afford to Trip

Source: https://www.wsj.com/articles/nvidia-is-winning-ai-race-but-cant-afford-to-trip-10d9e75b?mod=Searchresults_pos5&page=1

From the Article: "Chip maker's stock near record valuation as it extends lead even further with generative AI developments"

Biden, Trudeau Tout Job Boosts From Clean Energy, Chips Manufacturing

Source: https://www.wsj.com/articles/biden-trudeau-tout-job-boosts-from-clean-energy-

chips-manufacturing-c75ebfb0?mod=Searchresults_pos6&page=1

From the Article: "Two leaders also stress commitment to Ukraine in remarks to Canadian Parliament"

Watch: TikTok CEO Faces Off With Lawmakers Over Security Concerns

Source: https://www.wsj.com/video/watch-tiktok-ceo-faces-off-with-lawmakers-over-security-concerns/292A050C-79F5-4467-900B-E7854799C3D6.html?mod=Searchresults_pos8&page=1

From the Article: "TikTok CEO Shou Zi Chew responded to lawmakers' questions on Thursday about security concerns and potential Chinese government influence over the company. "

U.S. Companies Reshored 364,000 Jobs Last Year, Report Says

Source: https://www.wsj.com/livecoverage/stock-market-news-today-03-23-2023/card/u-s-companies-reshored-364-000-jobs-last-year-report-says-HOBgp4ivbIvZ32FRHgFC?mod=Searchresults_pos9&page=1

From the Article: "American companies reshored more jobs than expected from overseas last year, according to a report to be published Friday by the Reshoring Initiative. The organization, a nonprofit that tracks data aimed at encouraging companies to bring foreign jobs back to the U.S., said a record 364,000 jobs were reshored last year."

Toshiba Plans to Go Private in $15 Billion Deal With Japan Investors

Source: https://www.wsj.com/articles/toshiba-announces-15-billion-plan-to-be-taken-private-b090f9fb?mod=Searchresults_pos11&page=1

From the Article: "After tensions with foreign shareholders, company seeks new start under full domestic ownership"

Investors Just Can't Get Enough of Tech

Link back to Table of Contents

Source: https://www.wsj.com/livecoverage/stock-market-news-today-03-20-2023/card/investors-just-can-t-get-enough-of-tech-XfxUks6VURAq3KUrng9L?mod=Searchresults_pos12&page=1

From the Article: "Semiconductor companies have been big winners. Chip funds have had the highest amount of inflows when compared with other major technology sector fund groups, according to EPFR. The Philadelphia Semiconductor Index has added 20% this year, compared to a 2.8% gain for the S&P 500."

WSJ News Exclusive | Loophole Allows U.S. Tech Exports to Banned Chinese Firms

Source: https://www.wsj.com/articles/loophole-allows-u-s-tech-exports-to-banned-chinese-firms-b4800164?mod=Searchresults_pos14&page=1

From the Article: "Suppliers can sell to unlisted subsidiaries of companies on Commerce Department list, officials say"

Government Backing for Clean-Energy Startups May Replace Silicon Valley Bank Loans

Source: https://www.wsj.com/articles/government-backing-for-clean-energy-startups-may-replace-silicon-valley-bank-loans-ee4ae9e5?mod=Searchresults_pos17&page=1

From the Article: "Federal grants may be better suited than bank loans to support clean-energy innovation, industry advisers say"

The Winners and Losers if the U.S. Bans TikTok

Source: https://www.wsj.com/articles/the-winners-and-losers-if-the-u-s-bans-tiktok-e1690bf8?mod=Searchresults_pos18&page=1

From the Article: "From U.S.-China relations, to the parents of phone-addicted teenagers, the victims and beneficiaries run the gamut if TikTok disappears."

China's Xi Jinping Meets With Putin in Moscow as Beijing Casts Itself as Peacemaker

Source: https://www.wsj.com/articles/chinas-xi-arrives-in-moscow-as-beijing-seeks-to-position-itself-as-a-peacemaker-8f11d364?mod=Searchresults_pos1&page=2

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: "Fighting for battlefield advantage, neither Russia nor Ukraine is interested in talks now"

It Wasn't Just Credit Suisse. Switzerland Itself Needed Rescuing.

Source: https://www.wsj.com/articles/ubs-credit-suisse-rescue-switzerland-banks-36abe8c4?mod=Searchresults_pos5&page=2

From the Article: "Crisis threatened an economic model and national identity built on safeguarding the world's wealth"

What's Next for UBS After Rescue of Credit Suisse - What's News - WSJ Podcasts

Source: https://www.wsj.com/podcasts/whats-news/whats-next-for-ubs-after-rescue-of-credit-suisse/91914174-c81e-4347-a643-f2542b801544?mod=Searchresults_pos6&page=2

From the Article: "Swiss lender UBS has one fewer rival and more clients among the world's wealthy after its whirlwind rescue of Credit Suisse. But it's also left holding Credit Suisse's legal baggage and bearing the weight of being an even more systemically important financial institution."

Countries Compete to Lure Manufacturers From China

Source: https://www.wsj.com/articles/countries-compete-to-lure-manufacturers-from-china-adf46d9a?mod=Searchresults_pos10&page=1

From the Article: "Executives are looking for alternatives to China's vast factory floor—and governments are welcoming them"

Nvidia Is Winning AI Race, but Can't Afford to Trip

Source: https://www.wsj.com/articles/nvidia-is-winning-ai-race-but-cant-afford-to-trip-10d9e75b?mod=Searchresults_pos12&page=1

From the Article: "Chip maker's stock near record valuation as it extends lead even

Link back to Table of Contents

further with generative AI developments"

Xi and Putin Rekindle 'Strategic Bromance' in Russia

Source: https://www.wsj.com/articles/xi-and-putin-rekindle-strategic-bromance-in-russia-5f9f96dd?mod=Searchresults_pos14&page=1

From the Article: "Chinese leader gives apparent re-election endorsement to Russian president"

India's EV Dreams Face a Reality Check

Source: https://www.wsj.com/articles/indias-ev-dreams-face-a-reality-check-bda1db82?mod=Searchresults_pos8&page=1

From the Article: "Forcing manufacturers to use local components could backfire without a larger market—and other changes"

Ford Says It Will Lose $3 Billion on EVs This Year as It Touts Startup Mentality

Source: https://www.wsj.com/articles/ford-projects-3-billion-loss-on-ev-business-for-2023-98037e4e?mod=Searchresults_pos16&page=1

From the Article: "Company's estimate shows how far traditional auto makers have to go to make EV portfolios profitable"

Electric-Vehicle Growth Expands GM Cyber Chief's Concerns to Charging Stations

Source: https://www.wsj.com/articles/electric-vehicle-growth-expands-gm-cyber-chiefs-concerns-to-charging-stations-4f051e0e?mod=Searchresults_pos1&page=1

From the Article: "The shift from gasoline-powered vehicles is pushing the auto maker into electric infrastructure. Shielding that grid from cyberattacks will soon be part of Kevin Tierney's brief"

Link back to Table of Contents

Survey Finds Boards Have Work To Do on Cybersecurity: Executive Summary

Source: https://www.wsj.com/articles/survey-finds-boards-have-work-to-do-on-cybersecurity-executive-summary-6cf47acb?mod=Searchresults_pos2&page=1

From the Article: "Despite more than three-quarters of boards having at least one cyber expert among the directors, only three in 10 directors rate their board's ability to oversee a cyber crisis highly. More than one-third of directors representing the energy and utilities industry have no board cyber expert, highlighting vulnerability in the critical infrastructure sector."

European Ports Brace for Cybersecurity Regulation

Source: https://www.wsj.com/articles/european-ports-brace-for-cybersecurity-regulation-ece61a30?mod=Searchresults_pos3&page=1

From the Article: "A law taking effect in 2024 will require hundreds of companies at ports and in critical sectors to comply with cybersecurity rules for the first time"

Ukraine War Shows Difficulty of Large-Scale Cyberattacks, NSA Director Says

Source: https://www.wsj.com/articles/ukraine-war-shows-difficulty-of-large-scale-cyberattacks-nsa-director-says-b6bee3b3?mod=Searchresults_pos4&page=1

From the Article: "Gen. Paul Nakasone, in an interview, says U.S. rivals are trying to penetrate America's networks, data and weapons systems"

ChatGPT and Possible Cyber Benefits

Source: https://www.wsj.com/articles/chatgpt-and-possible-cyber-benefits-4cbc2d39?mod=Searchresults_pos5&page=1

From the Article: "ChatGPT is currently being used as a time-saving device, but the technology may hold potential for automating more complex tasks. The technology can be used to prepare well-crafted corporate messaging, provide policy writing support, develop realistic looking phishing emails and assist with identifying software 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.

Ferrari Investigating Cyber Incident

Source: https://www.wsj.com/articles/ferrari-investigating-cyber-incident-d39c0d47?mod=Searchresults_pos6&page=1

From the Article: "The auto company's Italian subsidiary was contacted with a ransom demand related to client contact details"

Opinion | Are We Headed for World War III?

Source: https://www.wsj.com/articles/are-we-headed-for-world-war-iii-china-russia-iran-electrical-infrastructure-ukraine-foreign-policy-b1b42224?mod=Searchresults_pos11&page=1

From the Article: "Students discuss the threat of China invading Taiwan, the war in Ukraine and polarizing domestic politics."

Those Pesky Password Rules Are Actually a Security Risk, Experts Say

Source: https://www.wsj.com/video/series/tech-news-briefing/those-pesky-password-rules-are-actually-a-security-risk-experts-say/9005A6B6-64D9-4C8B-B923-9A94B467B28E?mod=Searchresults_pos12&page=1

From the Article: "Cybersecurity researchers say systems that force users to change their passwords often actually could be creating security risks. But lots of companies and even government websites require this and other not-so-secure policies. WSJ tech columnist Christopher Mims joins host Zoe Thomas to discuss why security experts are concerned and the login strategies they suggest companies adopt."

Banks, Investors Revive Push for Changes to Securities Accounting After SVB Collapse

Source: https://www.wsj.com/articles/banks-investors-revive-push-for-changes-to-securities-accounting-after-svb-collapse-99caa9ce?mod=Searchresults_pos16&page=1

From the Article: "The Financial Accounting Standards Board after the financial crisis weighed fair-value requirements for financial institutions that planned to never sell their debt securities, but reversed course amid widespread industry objections"

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.

WSJ News Exclusive | Pentagon Probes Why Boeing Staff Worked on Air Force One Planes Without Security Credentials

Source: https://www.wsj.com/articles/pentagon-probes-lapse-in-boeing-security-credentials-for-air-force-one-163e0703?mod=Searchresults_pos18&page=1

From the Article: "About 250 Boeing workers had expired credentials that are needed to work on highly classified presidential jets"

How the Potential Arrest of Donald Trump Could Unfold

Source: https://www.wsj.com/articles/how-a-potential-indictment-and-arrest-of-donald-trump-could-unfold-456b06d5?mod=Searchresults_pos6&page=2

From the Article: "Security issues could affect any detention and court appearance involving the former president"

TikTok Fight Rocks U.S.-China Relations

Source: https://www.wsj.com/articles/tiktok-ban-ceo-congress-hearing-4bca3e2a?mod=Searchresults_pos16&page=2

From the Article: "Lawmakers press app's CEO over Chinese ties at tumultuous hearing"

A TikTok Ban May Be Just the Beginning

Source: https://www.wsj.com/articles/a-tiktok-ban-may-be-just-the-beginning-3ff8f081?mod=Searchresults_pos2&page=3

From the Article: "If the video app is blocked by federal authorities, it could be the beginning of the end for mega-popular Chinese apps in the U. S.—and for China's ambitions to build a software-driven economy"

TikTok Stars Rally in Washington Against App's Potential U.S. Ban

Source: https://www.wsj.com/articles/tiktok-stars-mount-washington-blitz-against-u-s-

Link back to Table of Contents

ban-f6d7834?mod=Searchresults_pos7&page=3

From the Article: "Firm enlists influencers for lobbying blitz before CEO's congressional testimony on Thursday"

ChatGPT Helped Win a Hackathon

Source: https://www.wsj.com/articles/chatgpt-helped-win-a-hackathon-96332de4?mod=Searchresults_pos15&page=3

From the Article: "A team from cybersecurity firm Claroty used the AI bot to write code to exploit vulnerabilities in industrial systems"

China Hits Back on TikTok, Says It Doesn't Ask Companies for Foreign Data

Source: https://www.wsj.com/articles/china-hits-back-on-tiktok-says-it-doesnt-ask-companies-for-foreign-data-e0cd6d84?mod=Searchresults_pos16&page=3

From the Article: "China's Foreign Ministry accuses the U.S. of suppressing the popular app"

Putin Proves an Unpredictable Partner for Xi as Nations Cement Ties

Source: https://www.wsj.com/articles/putin-proves-an-unpredictable-partner-for-xi-as-nations-cement-ties-184c083f?mod=Searchresults_pos11&page=4

From the Article: "Chinese leader's leverage over the Russian president isn't as clear-cut as it might seem"

China Is Starting to Act Like a Global Power

Source: https://www.wsj.com/articles/china-has-a-new-vision-for-itself-global-power-da8dc559?mod=Searchresults_pos11&page=5

From the Article: "Beijing grows bolder in challenging the U.S.-led global order"

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.

Debt Grows More Expensive, Harder to Get for Startups After SVB Collapse

Source: https://www.wsj.com/articles/debt-grows-more-expensive-harder-to-get-for-startups-after-svb-collapse-22a02cee?mod=Searchresults_pos2&page=7

From the Article: "Big banks are 'out of touch' with the lending needs of venture-backed startups, one investor says"

At the China-Russia Border, the Xi-Putin Partnership Shows Signs of Fraying

Source: https://www.wsj.com/articles/putin-xi-russia-china-ukraine-5c588831?mod=Searchresults_pos7&page=7

From the Article: "The meeting between the two leaders this week is expected to showcase unity, but a view of cities along the border reveals divisions that challenge the relationship"

Time to Curb Climate Change's Worst Effects Is Running Out, U.N. Panel Says - Minute Briefing - WSJ Podcasts

Source: https://www.wsj.com/podcasts/minute-briefing/time-to-curb-climate-changes-worst-effects-is-running-out-un-panel-says/3e2eb66a-9339-4988-ad99-930764597c45?mod=Searchresults_pos15&page=7

From the Article: "Plus: Ukraine says Russia is struggling to regain its initiative in the war amid heavy losses. The Federal Reserve first raised concerns about Silicon Valley Bank's risk management in 2019, documents show. J.R. Whalen reports."

How European Regulators Are Thinking About Emerging Tech - Tech News Briefing - WSJ Podcasts

Source: https://www.wsj.com/podcasts/tech-news-briefing/how-european-regulators-are-thinking-about-emerging-tech/4536efde-3b90-4e40-a901-a0f482d2cf96?mod=Searchresults_pos5&page=8

From the Article: "As more new technologies like artificial intelligence and the metaverse become mainstream, how are European Union officials approaching regulation? Spain's Secretary of State for Digitization and Artificial Intelligence Carme Artigas spoke about that with WSJ senior personal tech columnist Joanna Stern at this year's MWC. Julie

Link back to Table of Contents

Chang hosts."

Small Businesses Stress-Test Their Banks After Silicon Valley Bank's Collapse

Source: https://www.wsj.com/articles/small-businesses-stress-test-their-banks-after-silicon-valley-banks-collapse-a8844946?mod=Searchresults_pos10&page=8

From the Article: "Some entrepreneurs ask tough questions or shift deposits"

Fed Raises Rates but Nods to Greater Uncertainty After Banking Stress

Source: https://www.wsj.com/articles/fed-raises-rates-but-nods-to-greater-uncertainty-after-banking-stress-6ae9316f?mod=Searchresults_pos4&page=9

From the Article: "Officials voted unanimously to increase their benchmark short-term rate by a quarter percentage point"

Bank Failures Train Spotlight on Shortcomings in Risk Management

Source: https://www.wsj.com/articles/bank-failures-train-spotlight-on-shortcomings-in-risk-management-79765579?mod=Searchresults_pos14&page=10

From the Article: "Bank boards have risk committees tasked with forestalling problems. But the members of those committees don't always have the skills or stature to make themselves heard"

Opinion | The Chinese Communist Party's Plan A to Take Taiwan

Source: https://www.wsj.com/articles/the-chinese-communist-partys-plan-b-to-take-taiwan-jinping-united-front-influence-invasion-weapons-1653cc84?mod=Searchresults_pos20&page=10

From the Article: "Infiltrating, intimidating and co-opting the opposition would be less costly than an invasion."

Link back to Table of Contents

New X-Ray Checkpoints Scan for Fentanyl in Trucks at Mexico Border

Source: https://www.wsj.com/articles/fentanyl-opioid-us-mexico-border-5f947de?mod=Searchresults_pos12&page=12

From the Article: "Cartels rely on low probability of detection at crossings"

Companies Big and Small Lose Access to Credit Amid Bank Stress

Source: https://www.wsj.com/articles/companies-big-and-small-lose-access-to-credit-amid-bank-stress-53df944e?mod=Searchresults_pos18&page=12

From the Article: "Treasury market volatility keeps companies on sidelines during normally busy time for corporate debt financings"

SVB Collapse Shows Smaller Banks Can Pose Risk in Numbers

Source: https://www.wsj.com/articles/svb-collapse-shows-smaller-banks-can-pose-risk-in-numbers-4c676894?mod=Searchresults_pos19&page=12

From the Article: "Former regulators say Washington has been too focused on ‘too big to fail’ banks"

TikTok’s Chinese Parent Has Another Wildly Popular App in the U.S.

Source: https://www.wsj.com/articles/tiktoks-chinese-parent-has-another-wildly-popular-app-in-the-u-s-e14c41fc?mod=Searchresults_pos4&page=13

From the Article: "CapCut, the video-editing tool from ByteDance, helps users go viral on TikTok, Instagram and YouTube"

What Does ‘Made in America’ Mean? In Green Energy, Billions Hinge on the Answer

Source: https://www.wsj.com/articles/what-does-made-in-america-mean-in-green-energy-billions-hinge-on-the-answer-6e2471c5?mod=Searchresults_pos5&page=1

From the Article: "Companies pursuing subsidies try to shape the Treasury

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.

Department’s definition"

South Korea’s LG Energy to Build $5.6 Billion Battery Plant in Arizona

Source: https://www.wsj.com/articles/south-koreas-lg-energy-to-build-5-6-billion-battery-plant-in-arizona-b8abfa1d?mod=Searchresults_pos18&page=1

From the Article: "Company is the latest foreign battery maker to commit to projects tapping into the energy transition"

Freight Rebound Hopes Are Fading Under an Inventory Glut

Source: https://www.wsj.com/articles/freight-rebound-hopes-are-fading-under-an-inventory-glut-912995d2?mod=Searchresults_pos19&page=1

From the Article: "Logistics companies are paring back their expectations for a demand surge as retailers keep new orders in check"

Chinese Pressure Tactics Against Other Countries Largely Ineffective, Study Finds

Source: https://www.wsj.com/articles/chinese-pressure-tactics-against-other-countries-largely-ineffective-study-finds-3f49561f?mod=Searchresults_pos4&page=2

From the Article: "Trade restrictions sometimes produce the opposite of what Beijing wants, says Washington think tank"

Apple’s Tim Cook Upbeat in Beijing as China Courts Global CEOs

Source: https://www.wsj.com/articles/apples-tim-cook-upbeat-in-beijing-as-china-courts-global-ceos-373a6ff?mod=Searchresults_pos7&page=2

From the Article: "Business leaders and Chinese officials at economic forum are careful to tiptoe around Sino-U.S. political ties"

Big Oil Eyes New Deals in North Africa - The Wall Street Journal Google Your News

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.

Update - WSJ Podcasts

Source: https://www.wsj.com/podcasts/google-news-update/big-oil-eyes-new-deals-in-north-africa/9c336254-aa92-4dcc-b558-04cfaceed4d6?mod=Searchresults_pos8&page=3

From the Article: "North Africa is catching the attention of big oil companies, as energy demand from Europe grows following Russia's invasion of Ukraine. The Wall Street Journal's North Africa correspondent Chao Deng joins WSJ What's News host Annmarie Fertoli to discuss. "

Joe Biden's Push to Counter China Steers EV Investments to Canada

Source: https://www.wsj.com/articles/joe-bidens-push-to-counter-china-steers-ev-investments-to-canada-a3095936?mod=Searchresults_pos14&page=3

From the Article: "Volkswagen Group, Brazilian miner Vale and others are investing billions of dollars in the country's electric-vehicle and mining sectors"

I Saw the Face of God in a Semiconductor Factory

Source: https://www.wired.com/story/i-saw-the-face-of-god-in-a-tsmc-factory/

From the Article: "As the US boosts production of silicon chips, an American journalist goes inside TSMC, the mysterious Taiwanese company at the center of the global industry."

Security News This Week: Ring Is in a Standoff With Hackers - WIRED

Source: https://www.wired.com/story/amazon-ring-hacked-ransomware/

From the Article: "What's more controversial than a popular surveillance camera maker that has an uncomfortably cozy relationship with American police? When ransomware hackers claim to have breached that company—Amazon-owned camera maker Ring—stolen its data, and Ring responds by denying the breach."

India Shut Down Cell Service for 27 Million During a Manhunt

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.wired.com/story/india-activist-manhunt-sikh-activist/

From the Article: "Plus: The “Clop” gang’s ransomware spree, the DC Health Link breach comes into focus, and more."

The Top Five Cybersecurity Concerns - Forbes

Source: https://www.forbes.com/sites/forbestechcouncil/2023/03/20/the-top-five-cybersecurity-concerns/

From the Article: "Cybersecurity will continue to be an ongoing concern for organizations, especially with cyber threats continuing to grow more intense alongside our increasing reliance on software for business functions."

Medicare Ransomware Attack Details Sought by GOP Committee Heads

Source: https://news.bloomberglaw.com/privacy-and-data-security/medicare-ransomware-attack-details-sought-by-gop-committee-heads

From the Article: "Republican congressional leaders want the US Centers for Medicare and Medicaid Services to turn over more information on a ransomware attack that exposed the identifiable information of 254,000 Medicare beneficiaries."

Ferrari Says Ransomware Attack Exposed Clients' Names, Email - BNN Bloomberg

Source: https://www.bloomberg.com/news/articles/2023-03-20/ferrari-says-ransomware-attack-exposed-clients-names-email

From the Article: "No payment details, bank account numbers or details of Ferrari cars owned or ordered were stolen, and the breach has had no impact on the operations of the carmaker, Vigna added."

Taiwan braces for drought in key chip hubs again

Source: https://asia.nikkei.com/Business/Business-Spotlight/Taiwan-braces-for-drought-in-key-chip-hubs-again

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: "Water challenge comes as island pushes to maintain 'silicon shield' against China"

China's Triniti targets $290m fund to back chip companies

Source: https://asia.nikkei.com/Spotlight/DealStreetAsia/China-s-Triniti-targets-290m-fund-to-back-chip-companies

From the Article: "Fund also has mandate to invest in display technologies and new energy"

Japan officially lifts South Korea trade curbs, as ties warm

Source: https://asia.nikkei.com/Spotlight/Japan-South-Korea-rift/Japan-officially-lifts-South-Korea-trade-curbs-as-ties-warm

From the Article: "Seoul concurrently withdraws WTO dispute settlement"

EV price war in Thailand heats up as Bangkok Motor Show commences

Source: https://asia.nikkei.com/Business/Automobiles/EV-price-war-in-Thailand-heats-up-as-Bangkok-Motor-Show-commences

From the Article: "BYD and Hyundai push new models as kingdom's auto sales decline"

China can sway chip markets without overtaking U.S.: Chris Miller

Source: https://asia.nikkei.com/Business/Tech/Semiconductors/China-can-sway-chip-markets-without-overtaking-U.S.-Chris-Miller

From the Article: "'Chip War' author says Beijing's policies can impact global semiconductor industry"

U.S. readies targeted screening for investment in Chinese tech

Source: https://asia.nikkei.com/Politics/International-relations/U.S.-readies-targeted-

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.

screening-for-investment-in-Chinese-tech

From the Article: "Narrower 'reverse CFIUS' to focus on areas like chips and quantum computing"

U.S. seeks to block Beijing from $52bn chips funding benefits

Source: https://asia.nikkei.com/Spotlight/Supply-Chain/U.S.-seeks-to-block-Beijing-from-52bn-chips-funding-benefits

From the Article: "Proposal limits investing in production expansion in China or Russia"

Link back to Table of Contents