Weekly Security Articles 06-April-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.

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

Setting Yourself Up for SUCCESS Manual DMSMS

Source:
https://www.dau.edu/event/Setting_Yourself_Up_for_SUCCESS_Manual_DMSMS

April 20,2023

Live Webinar | Creating Trust in an Insecure World: Strategies for CISOs in the Age of Increasing Vulnerabilities

Source: https://www.bankinfosecurity.com/webinars/live-webinar-creating-trust-in-insecure-world-strategies-for-cisos-in-w-4774

May 17, 2023

Live Webinar | Education Cybersecurity Best Practices: Devices, Ransomware, Budgets and ...

Source: https://www.bankinfosecurity.com/webinars/live-webinar-education-cybersecurity-best-practices-devices-ransomware-w-4772

May 24, 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.

Events - In-person

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

CHIPS for America Vision for Success 2023 Policy and Strategy Summit - Purdue University Semiconductors

Source: https://engineering.purdue.edu/semiconductors/news/development-summit

April 18, 2023

RSA Conference

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

Cyber Week

Source: https://cyberweek.tau.ac.il/2023/

June 26-29, 2023

Symposium on Counterfeit Parts and Materials

Source: https://smta.org/mpage/counterfeit

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.

June 27-29, 2023

.conf22 User Conference | Splunk

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

July 17-20, 2023

Black Hat

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

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

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.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.

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

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.

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

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

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

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.

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

ANSI Draft Roadmap of Standards and Codes for Electric Vehicles at Scale Released for Comment

Source: https://www.ansi.org/news/standards-news/all-news/2023/03/3-31-23-ansi-draft-roadmap-of-standards-and-codes-for-electric-vehicles-at-scale-released

From the Article: "The American National Standards Institute (ANSI) released today for public review and comment a draft of the Roadmap of Standards and Codes for Electric Vehicles at Scale developed by the Institute's Electric Vehicles Standards Panel (EVSP). The roadmap identifies key safety, performance, and interoperability issues; notes relevant published and in-development standards; and makes recommendations to address gaps in codes and standards."

Comments due: May 1, 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

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: "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-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-

Link back to Table of Contents

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

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

Apple Releases Security Updates for Multiple Products

https://www.cisa.gov/news-events/alerts/2023/03/28/apple-releases-security-updates-multiple-products

SAFECOM Publishes Updated SAFECOM Fact Sheet

https://www.cisa.gov/news-events/news/safecom-publishes-updated-safecom-fact-sheet

CISA Releases One Industrial Control Systems Advisory

https://www.cisa.gov/news-events/alerts/2023/03/30/cisa-releases-one-industrial-

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.

control-systems-advisory

Hitachi Energy IEC 61850 MMS-Server

https://www.cisa.gov/news-events/ics-advisories/icsa-23-089-01

Supply Chain Attack Against 3CXDesktopApp

https://www.cisa.gov/news-events/alerts/2023/03/30/supply-chain-attack-against-3cxdesktopapp

Review – 1 Advisory Published – 3-30-23

https://chemical-facility-security-news.blogspot.com/2023/03/review-1-advisory-published-3-30-23.html

CISA Adds Ten Known Exploited Vulnerabilities to Catalog

https://www.cisa.gov/news-events/alerts/2023/03/30/cisa-adds-ten-known-exploited-vulnerabilities-catalog

Samba Releases Security Updates for Multiple Versions of Samba

https://www.cisa.gov/news-events/alerts/2023/03/31/samba-releases-security-updates-multiple-versions-samba

Mozilla Releases Security Update for Thunderbird 102.9.1

https://www.cisa.gov/news-events/alerts/2023/03/31/mozilla-releases-security-update-thunderbird-10291

Review – Public ICS Disclosures – Week of 3-25-23

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://chemical-facility-security-news.blogspot.com/2023/04/review-public-ics-disclosures-week-of-3.html

Patches/Advisories Articles of Interest

Microsoft Fixes New Azure AD Vulnerability Impacting Bing Search and Major Apps

Source: https://thehackernews.com/2023/04/microsoft-fixes-new-azure-ad.html

From the Article: "Microsoft has patched a misconfiguration issue impacting the Azure Active Directory (AAD) identity and access management service that exposed several "high-impact" applications to unauthorized access."

Technical Analysis of Windows CLFS Zero-Day Vulnerability CVE-2022-37969 - Part 1: Root Cause Analysis

Source: https://www.zscaler.com/blogs/security-research/technical-analysis-windows-clfs-zero-day-vulnerability-cve-2022-37969-part

From the Article: "On September 2, 2022, Zscaler Threatlabz captured an in-the-wild 0-day exploit in the Windows Common Log File System Driver (CLFS.sys) and reported this discovery to Microsoft. In the September Tuesday patch, Microsoft fixed this vulnerability that was identified as CVE-2022-37969, which is a Windows Common Log File System Driver elevation of privilege vulnerability."

CVE-2023-1800

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-1800

From the Article: "A vulnerability, which was classified as critical, has been found in sjqzhang go-fastdfs up to 1.4.3. Affected by this issue is the function upload of the file /group1/uploa of the component File Upload Handler. "

CVE-2023-1793

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-1793

From the Article: "A vulnerability was found in SourceCodester Police Crime Record Management System 1.0. It has been classified as critical. This affects an unknown part

of the file /officer/assigncase.php of the component GET Parameter Handler."

CVE-2023-0187

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-0187

From the Article: "NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer handler, where an out-of-bounds read can lead to denial of service."

CVE-2023-0188

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-0188

From the Article: "NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer handler, where an unprivileged user can cause improper restriction of operations within the bounds of a memory buffer cause an out-of-bounds read, which may lead to denial of service."

CISA adds bugs exploited by commercial surveillance spyware to Known Exploited Vulnerabilities catalog

Source: https://securityaffairs.com/144315/breaking-news/cisa-known-exploited-vulnerabilities-catalog-spyware-bugs.html

From the Article: "CISA has added nine flaws to its Known Exploited Vulnerabilities catalog, including bugs exploited by commercial spyware on mobile devices."

Threat Advisory: 3CX Softphone Supply Chain Compromise

Source: https://blog.talosintelligence.com/3cx-softphone-supply-chain-compromise/

From the Article: "Cisco Talos recently became aware of a supply chain attack affecting Windows and MacOS users of the 3CX software-based phone application. This attack leveraged the legitimate update functionality of the 3CX application to deliver a set of malicious payloads to 3CX users."

Link back to Table of Contents

Vulnerability Spotlight: Vulnerability in ManageEngine OpManager could lead to XXE attack

Source: https://blog.talosintelligence.com/vulnerability-spotlight-vulnerability-in-manageengine-opmanager-could-lead-to-xxe-attack/

From the Article: "OpManager is network monitoring software that allows users to track and manage the performance of connected routers, switches, firewalls, servers, VMs and more. A vulnerability (TALOS-2022-1685/CVE-2022-43473) exists when the user attempts to add a unified computing system (UCS) to the software."

WordPress WooCommerce 7.1.0 Remote Code Execution

Source: https://packetstormsecurity.com/files/171609/wpwoocommerce710-exec.txt

From the Article: "WordPress WooCommerce plugin version 7.1.0 suffers from a remote code execution vulnerability."

Textpattern 4.8.8 Remote Code Execution

Source: https://packetstormsecurity.com/files/171607/textpattern488-exec.txt

From the Article: "Textpattern version 4.8.8 suffers from an authenticated remote code execution vulnerability."

New Azure Flaw "Super FabriXss" Enables Remote Code Execution Attacks

Source: https://www.infosecurity-magazine.com/news/new-azure-flaw-fabrixss-enables-rce/

From the Article: "The cross-site scripting flaw affects SFX version 9.1.1436.9590 or earlier and has a CVSS of 8.2."

CONPROSYS HMI System(CHS) vulnerable to SQL injection

Source: https://jvn.jp/en/vu/JVNVU92145493/

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: "CONPROSYS HMI System(CHS) provided by Contec Co., Ltd. contains an SQL injection vulnerability."

Multiple vulnerabilities in Seiko Solutions SkyBridge MB-A100/A110/A200/A130 SkySpider MB-R210

Source: https://jvn.jp/en/jp/JVN40604023/

From the Article: "SkyBridge MB-A100/A110/A200/A130 SkySpider MB-R210 provided by Seiko Solutions Inc. contain multiple vulnerabilities."

CISA Warns of Vulnerabilities in Propump and Controls' Osprey Pump Controller

Source: https://www.hackread.com/cisa-vulnerability-propump-osprey-pump-controller/

From the Article: "CISA's advisory came after the Macedonian cybersecurity firm Zero Science Lab discovered and reported the vulnerabilities to authorities."

Patch Now: Cybercriminals Set Sights on Critical IBM File Transfer Bug

Source: https://www.darkreading.com/vulnerabilities-threats/patch-now-cybercriminals-set-sights-critical-ibm-file-transfer-bug

From the Article: "A vulnerability with a 9.8 CVSS rating in IBM's widely deployed Aspera Faspex offering is being actively exploited to compromise enterprises."

Ransomware gangs are exploiting IBM Aspera Faspex RCE flaw (CVE-2022-47986)

Source: https://www.helpnetsecurity.com/2023/03/30/exploiting-cve-2022-47986/

From the Article: "Attackers are exploiting a critical vulnerability (CVE-2022-47986) in the IBM Aspera Faspex centralized file transfer solution to breach organizations. "

CVE-2023-25076

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://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-25076

From the Article: " An attacker could send a malicious packet to trigger this vulnerability."

Remove Hairysquid ransomware (virus) - Recovery Instructions Included - 2-Spyware.com

Source: https://www.2-spyware.com/remove-hairysquid-ransomware.html

From the Article: "Hairysquid ransomware is a file-locking virus that infects computers and encrypts users' personal files, such as photos, videos, and documents. It is a Mimic ransomware variant."

Apple patches all the iThings, including iOS 15 hole under attack right now

Source: https://www.theregister.com/2023/03/28/apple_patches_iphone/

From the Article: "Happy belated Patch Tuesday from Cupertino: Apple has issued security updates for almost every piece of code it slings - including a fix for a vulnerability in older iOS devices the iGiant believes is under attack right now."

Microsoft Issues Patch for aCropalypse Privacy Flaw in Windows Screenshot Tools

Source: https://thehackernews.com/2023/03/microsoft-issues-patch-for-acropalypse.html

From the Article: "Microsoft has released an out-of-band update to address a privacy-defeating flaw in its screenshot editing tool for Windows 10 and Windows 11."

iOS Security Update Patches Exploited Vulnerability in Older iPhones

Source: https://www.securityweek.com/ios-security-update-patches-exploited-vulnerability-in-older-iphones/

From the Article: "Apple has released security updates for older iPhones to address a vulnerability exploited in 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.

Vulnerability Spotlight: Specially crafted files could lead to denial of service, information disclosure in OpenImageIO parser

Source: https://blog.talosintelligence.com/vulnerability-spotlight-specially-crafted-files-could-lead-to-denial-of-service-information-disclosure-in-openimageio-parser/

From the Article: "Cisco Talos recently discovered three vulnerabilities in the OpenImageIO image-parsing library that many popular pieces of 3-D rendering software use."

Vulnerability Spotlight: SNIProxy contains remote code execution vulnerability

Source: https://blog.talosintelligence.com/vulnerability-spotlight-sniproxy-contains-remote-code-execution-vulnerability/

From the Article: "Cisco ASIG recently discovered a remote code execution vulnerability in the SNIProxy open-source tool that occurs when the user utilizes wildcard backend hosts."

Apple backports fix for exploited WebKit bug to older iPhones, iPads (CVE-2023-23529)

Source: https://www.helpnetsecurity.com/2023/03/28/cve-2023-23529-older-iphones-ipads/

From the Article: "Apple has released security updates for – pardon the pop-culture reference – everyhing everywhere all at once, and has fixed the WebKit vulnerability (CVE-2023-23529) exploited in the wild for users of older iPhones and iPads."

SolarWinds Information Service (SWIS) Remote Command Execution

Source: https://packetstormsecurity.com/files/171567/solarwinds_amqp_deserialization.rb.txt

From the Article: "The SolarWinds Information Service (SWIS) is vulnerable to remote code execution by way of a crafted message received through the AMQP message queue."

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.

MS-ISAC CYBERSECURITY ADVISORY - Multiple Vulnerabilities in Adobe Products Could Allow for Arbitrary Code Execution

Source: https://www.cisecurity.org/advisory/ms-isac-cybersecurity-advisory---multiple-vulnerabilities-in-adobe-products-could-allow-for-arbitrary-code-execution_2023-031

From the Article: "Multiple vulnerabilities have been discovered in Adobe products, the most severe of which could allow for arbitrary code execution."

SolarWinds Information Service (SWIS) Remote Command Execution

Source: https://packetstormsecurity.com/files/171567/solarwinds_amqp_deserialization.rb.txt

From the Article: "The SolarWinds Information Service (SWIS) is vulnerable to remote code execution by way of a crafted message received through the AMQP message queue."

BoxBilling 4.22.1.5 Remote Code Execution

Source: https://packetstormsecurity.com/files/171542/boxbilling42215-exec.txt

From the Article: "BoxBilling versions 4.22.1.55 and below suffer from a remote code execution vulnerability."

Suprema BioStar 2 2.8.16 SQL Injection

Source: https://packetstormsecurity.com/files/171523/supremabiostar2816-sql.txt

From the Article: "Suprema BioStar 2 version 2.8.16 suffers from a remote SQL injection vulnerability."

WebTareas 2.4 SQL Injection

Source: https://packetstormsecurity.com/files/171521/webtareas24unauth-sql.txt

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: "WebTareas version 2.4 suffers from a remote blind SQL injection vulnerability. Original discovery of this issue in this version is attributed to Behrad Taher in May of 2022."

WebTareas 2.4 Cross Site Scripting

Source: https://packetstormsecurity.com/files/171520/webtareas24-xss.txt

From the Article: "WebTareas version 2.4 suffers from multiple cross site scripting vulnerabilities."

Fortinet 7.2.1 Authentication Bypass

Source: https://packetstormsecurity.com/files/171515/forti721-bypass.txt

From the Article: "Fortinet FortiOS, FortiProxy, and FortiSwitchManager version 7.2.1 suffers from a authentication bypass vulnerability."

CVE-2022-48353

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-48353

From the Article: "Some smartphones have configuration issues. Successful exploitation of this vulnerability may cause kernel privilege escalation, which results in system service exceptions."

Apple fixes recently disclosed CVE-2023-23529 zero-day on older devices

Source: https://securityaffairs.com/144114/hacking/cve-2023-23529-apple-zero-day.html

From the Article: "Apple released updates to backport security patches that address actively exploited CVE-2023-23529 WebKit zero-day for older iPhones and iPads."

Link back to Table of Contents

Microsoft Released an Update for Windows Snipping Tool Vulnerability, (Sat, Mar 25th)

Source: https://isc.sans.edu/diary/rss/29670

From the Article: "To exploit this vulnerability, the image must be created under very specific condition listed here."

Webgrind 1.1 Cross Site Scripting / Remote Code Execution

Source: https://packetstormsecurity.com/files/171501/webgrind11-xssexec.txt

From the Article: "Webgrind version 1.1 suffers from remote code execution and cross site scripting vulnerabilities."

WiFi Mouse 1.8.3.2 Remote Code Execution

Source: https://packetstormsecurity.com/files/171499/wifimouse1832-exec.txt

From the Article: "WiFi Mouse version 1.8.3.2 suffers from a remote code execution vulnerability."

eXtplorer 2.1.14 Authentication Bypass / Remote Code Execution

Source: https://packetstormsecurity.com/files/171493/extplorer2114-bypassexec.txt

From the Article: "eXtplorer version 2.1.14 suffers from authentication bypass and remote code execution vulnerabilities."

Composr-CMS 10.0.39 Remote Code Execution

Source: https://packetstormsecurity.com/files/171489/composrcms10039-exec.txt

From the Article: "Composr-CMS versions 10.0.39 and below suffer from an authenticated remote code execution vulnerability."

MODX Revolution 2.8.3-pl Remote Code Execution

Link back to Table of Contents

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

Source: https://packetstormsecurity.com/files/171488/modxrevolution283pl-exec.txt

From the Article: "MODX Revolution version 2.8.3-pl suffers from an authenticated remote code execution vulnerability."

Abantecart 1.3.2 Remote Code Execution

Source: https://packetstormsecurity.com/files/171487/abantecart132-exec.txt

From the Article: "Abantecart version 1.3.2 suffers from an authenticated remote code execution vulnerability."

SimpleMachinesForum 2.1.1 Remote Code Execution

Source: https://packetstormsecurity.com/files/171486/smf211-exec.txt

From the Article: "SimpleMachinesForum version 2.1.1 suffers from an authenticated remote code execution vulnerability."

Microsoft Offers Guidelines on Detecting Outlook Zero-day Exploits

Source: https://www.cysecurity.news/2023/03/microsoft-offers-guidelines-on.html

From the Article: "Microsoft has released a detailed guide to assist customers in detecting signs of compromise by exploiting a recently patched Outlook zero-day vulnerability. This privilege escalation security flaw in the Outlook client for Windows, tracked as CVE-2023-23397, enables attackers to steal NTLM hashes without user interaction in NTLM-relay zero-click attacks. "

D-Link DNR-322L 2.60B15 Remote Code Execution

Source: https://packetstormsecurity.com/files/171480/dlinkdnr322l-exec.txt

From the Article: "D-Link DNR-322L versions 2.60B15 and below suffer from an authenticated remote code execution vulnerability."

Link back to Table of Contents

OpenSSL 1.1.1 Nears End of Life: Security Updates Only Until September 2023

Source: https://www.securityweek.com/openssl-1-1-1-nears-end-of-life-security-updates-only-until-september-2023/

Summary: OpenSSL 1.1.1 is nearing end of life, security updates only available until Sept. 2023.

Podcasts/Videos

AI Can't Stop, Won't Stop; Early Stage Funding is Strong; YouTubers Hacked – ESW #311

Source: https://www.scmagazine.com/podcast-segment/ai-cant-stop-wont-stop-early-stage-funding-is-strong-youtubers-hacked-esw-311

Unpacking the White House National Cybersecurity Strategy – Josh Corman – ESW #311

Source: https://www.scmagazine.com/podcast-segment/unpacking-the-white-house-national-cybersecurity-strategy-josh-corman-esw-311

Trust, Autonomy, and Building Amazing Distributed Teams – Nick Means – ESW #311

Source: https://www.scmagazine.com/podcast-segment/trust-autonomy-and-building-amazing-distributed-teams-nick-means-esw-311

The RESTRICT Act, Intel's Attack Surface, & Stop Developing AI (For 6 Months) – PSW #778

Source: https://www.scmagazine.com/podcast-segment/the-restrict-act-intels-attack-surface-stop-developing-ai-for-6-months-psw-778

Simply Cyber: 🔴 March 31's Top Cyber News NOW! - Ep 335 on Apple Podcasts

Source: https://podcasts.apple.com/us/podcast/march-31s-top-cyber-news-now-ep-335/id1590662228?i=1000606804074

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 30's Top Cyber News NOW! - Ep 334 on Apple Podcasts

Source: https://podcasts.apple.com/us/podcast/march-30s-top-cyber-news-now-ep-334/id1590662228?i=1000606645801

Simply Cyber: 🔴 March 29's Top Cyber News NOW! - Ep 333 on Apple Podcasts

Source: https://podcasts.apple.com/us/podcast/march-29s-top-cyber-news-now-ep-333/id1590662228?i=1000606486204

Simply Cyber: 🔴 March 28's Top Cyber News NOW! - Ep 332 on Apple Podcasts

Source: https://podcasts.apple.com/us/podcast/march-28s-top-cyber-news-now-ep-332/id1590662228?i=1000606355125

Simply Cyber: 🔴 March 27's Top Cyber News NOW! - Ep 331 on Apple Podcasts

Source: https://podcasts.apple.com/us/podcast/march-27s-top-cyber-news-now-ep-331/id1590662228?i=1000606165755

7MS #566: Tales of Pentest Pwnage - Part 47

Source: https://7ms.us/7ms-566-tales-of-pentest-pwnage-part-47/

The Hacker Factory: From Developer to Cybersecurity Pro | A Conversation with Greg Porterfield | The Hacker Factory Podcast With Phillip Wylie on Apple Podcasts

Source: https://podcasts.apple.com/us/podcast/from-developer-to-cybersecurity-pro-a-conversation/id1581926992?i=1000606758054

Microsoft's Email Extortion | TWiT.TV

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://twit.tv/shows/security-now/episodes/916

NO. 375 | 6 Post-GPT Phases, Github's Private Key, New Assistant Interfaces

Source: https://danielmiessler.com/podcast/no-375/

Ep 237 | 3.30.23 Seeking employment fraud?

Source: https://thecyberwire.com/podcasts/hacking-humans/237/notes

315: Crypto hacker hijinks, government spyware, and Utah social media shocker

Source: https://www.smashingsecurity.com/315-crypto-hacker-hijinks-government-spyware-and-utah-social-media-shocker/

Ep 1792 | 3.31.23 A glimpse into Mr. Putin's cyber war room. 3CXDesktopAppsupply chain risk. XSS flaw in Azure SFX can lead to remote code execution. AlienFox targets misconfigured servers.

Source: https://thecyberwire.com/podcasts/daily-podcast/1792/notes

Ep 1791 | 3.30.23 A major supply chain attack is underway. Ms Connor, call your office. Combosquatting. False positives fixed. Tanks don't work, so Russia tries more cyber. And, sadly. some official hostage-taking.

Source: https://thecyberwire.com/podcasts/daily-podcast/1791/notes

Ep 1790 | 3.29.23 Traffers and the threat to credentials. WiFi protocol flaw. Cross-chain bridge attacks. A shift in Russian cyber operations. Piracy is patriotic.

Source: https://thecyberwire.com/podcasts/daily-podcast/1790/notes

Ep 1789 | 3.28.23 Twitter looks for a leaker. Insider risks. The state of resilience. Russian

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.

auxiliaries briefly disrupt a French National Assembly website. Cyber trends in the hybrid war. DPRK hacking, as it is.

Source: https://thecyberwire.com/podcasts/daily-podcast/1789/notes

Ep 1788 | 3.27.23 Evolution of criminal scams (especially BEC). Law enforcement honeypots. ChatGPT data leak. Hybrid war updates.

Source: https://thecyberwire.com/podcasts/daily-podcast/1788/notes

Risky Biz News: North Korean hackers behind supply chain attack on 3CX

Source: https://risky.biz/RBNEWS130/

Srsly Risky Biz: Army. Navy. Air Force. Cyber Force?

Source: https://risky.biz/SRB29/

Risky Biz News: White House bars federal agencies from using rogue commercial spyware

Source: https://risky.biz/RBNEWS129/

Risky Business #701 -- Why infosec is wrong about TikTok

Source: https://risky.biz/RB701/

Between Two Nerds: The Real Problem with TikTok

Source: https://risky.biz/BTN30/

Risky Biz News: CISA rolls out pre-ransomware notification system

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

Source: https://risky.biz/RBNEWS128/

Episode 52: Back in the Buzz of RSA Conference

Source: https://www.cisecurity.org/insights/podcast/episode-52-back-in-the-buzz-of-rsa-conference

To receive testimony on enterprise cybersecurity to protect the Department of Defense Information Networks | United States Senate Committee on Armed Services

Source: https://www.armed-services.senate.gov/hearings/to-receive-testimony-on-enterprise-cybersecurity-to-protect-the-department-of-defense-information-networks

Reshoring Jobs Hit All-Time High

Source: https://www.manufacturing.net/video/video/22793188/reshoring-jobs-hit-alltime-high

VLOG-201 | The #Semiconductor Better Chips

Source: https://www.youtube.com/watch?v=6hT2jaDrDbU

Funding for International Partnerships Through the CHIPS Act - United States Department of State

Source: https://www.state.gov/briefings-foreign-press-centers/funding-for-international-partnerships-through-the-chips-act

Understanding Xi Jinping's Digital Strategy for China - United States Department of State

Source: https://www.state.gov/briefings-foreign-press-centers/understanding-xi-jingings-digital-strategy-for-china

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.

Smashing Security podcast #315: Crypto hacker hijinks, government spyware, and Utah social media shocker

Source: https://grahamcluley.com/smashing-security-podcast-315/

From the Article: "A cryptocurrency hack leads us down a maze of twisty little passages, Joe Biden's commercial spyware bill, and Utah gets tough on social media sites."

Data breach NS rail. Latitude breach larger than initially thought. America the oversharing. Financial services company breach exposes credit card data.

Source: https://thecyberwire.com/podcasts/privacy-briefing/796/notes

From the Article: "Data breach derails Dutch national rail company. Latitude data breach far larger than initially thought. Strangers don't need to see more pics of your kids. Financial services company breach exposes credit card data."

Traffers and the threat to credentials. WiFi protocol flaw. Cross-chain bridge attacks. A shift in Russian cyber operations. Piracy is patriotic.

Source: https://thecyberwire.com/podcasts/daily-podcast/1790/notes

From the Article: "Traffers and the threat to credentials. A newly discovered WiFi protocol flaw. Cross-chain bridge attacks. A shift in Russian cyber operations. Ann Johnson from Afternoon Cyber Tea chats with EY principal Adam Malone."

Crown Resorts falls victim to the GoAnywhere leak. US hospital still struggling after 2021 data breach. Oakland police union says city mishandled recent data breach.

Source: https://thecyberwire.com/podcasts/privacy-briefing/795/notes

From the Article: "France bans TikTok (and then some) from government phones. Could a Cyber Force become the seventh arm of the US military? Biden administration restricts use of commercial surveillance software."

Twitter looks for a leaker. Insider risks. The state of resilience. Russian auxiliaries briefly disrupt a French National Assembly website. Cyber trends in the hybrid war. DPRK hacking, as it is.

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://thecyberwire.com/podcasts/daily-podcast/1789/notes

From the Article: "Twitter gets a subpoena for a source-code leaker's information. The insider risk to data. Russian hacktivist auxiliaries target the French National Assembly. Recent trends in cyberattacks sustained by Ukraine. Ben Yelin unpacks the White House executive order on spyware."

Video: How to Build Resilience Against Emerging Cyber Threats

Source: https://www.securityweek.com/video-how-to-build-resilience-against-emerging-cyber-threats/

From the Article: "Enjoy this session as we walk through three recent use cases where a new threat caught organizations off-guard."

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

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. Will discuss on 04/12/2023."

Prohibition on Certain Semiconductor Products and Services

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.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.”

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.”

Link back to Table of Contents

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."

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

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.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 05/03/2023"

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

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

Link back to Table of Contents

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, 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 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."

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.

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."

Reports - Government

Predetermined Change Control Plans for AI/ML-Enabled Device Functions

Source: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/marketing-submission-recommendations-predetermined-change-control-plan-artificial

Cybersecurity in Medical Devices: Refuse to Accept Policy for Cyber Devices and Related Systems Under Section 524B of the FD&C Act - Guidance for Industry and Food and Drug Administration Staff

Source: https://www.fda.gov/media/166614/download

https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity-medical-devices-frequently-asked-questions-faqs

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.fda.gov/medical-devices/medical-devices-news-and-events/cdrh-issues-draft-guidance-predetermined-change-control-plans-artificial-intelligencemachine

https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-refuse-accept-policy-cyber-devices-and-related-systems-under-section

Cyber Security Toolkit for Boards

Source: https://www.ncsc.gov.uk/collection/board-toolkit

National Security Agency | Cybersecurity Information Sheet - Advancing Zero Trust Maturity Throughout the User Pillar

Source: https://media.defense.gov/2023/Mar/14/2003178390/-1/-1/0/CSI_ZERO%20TRUST%20USER%20PILLAR.PDF

National quantum strategy
Source:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1142942/national_quantum_strategy.pdf

Reports - Industry

Upstream's 2023 Global Automotive Cybersecurity Report

Source: https://upstream.auto/reports/global-automotive-cybersecurity-report

UK Ransomware Trends: Lessons for 2023 | JUMPSEC

Source: https://www.jumpsec.com/uk-ransomware-trends-lessons-for-2023/

Internet Security Report - Q4 2022 | WatchGuard Technologies

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.watchguard.com/wgrd-resource-center/security-report-q4-2022

Risk Strategies - State of The Insurance Market Report 2023

Source: https://www.risk-strategies.com/2023-state-of-the-market

CANADA AND TAIWAN: A STRONG RELATIONSHIP IN TURBULENT TIMES

Interim Report of the Special Committee on the Canada– People's Republic of China Relationship

Source: https://www.ourcommons.ca/content/Committee/441/CACN/Reports/RP12317356/441_CACN_Rpt2_PDF/441_CACN_Rpt2-e.pdf

Sophos Threat Report

Source: https://www.sophos.com/en-us/content/security-threat-report

Semiconductor Industry 2023 Preview

Source: https://www.digitimes.com/topic/semiconductor_industry_2023_preview/a001609.html

U.S. Semiconductor Ecosystem Map

Source: https://www.semiconductors.org/u-s-semiconductor-ecosystem-map/

Semiconductors 20 2023 | The Annual Brand Value Ranking | Brandirectory

Source: https://brandirectory.com/rankings/semiconductors/

Salt Security: OWASP API Security Top 10 Explained

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://content.salt.security/wp-owasp-api-top-10

White House

FACT SHEET: Biden-Harris Administration Announces New Private and Public Sector Investments for Affordable Electric Vehicles | The White House

Source: https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/30/fact-sheet-biden-harris-administration-announces-new-private-and-public-sector-investments-for-affordable-electric-vehicles/

Executive Order on Prohibition on Use by the United States Government of Commercial Spyware that Poses Risks to National Security | The White House

Source: https://www.whitehouse.gov/briefing-room/presidential-actions/2023/03/27/executive-order-on-prohibition-on-use-by-the-united-states-government-of-commercial-spyware-that-poses-risks-to-national-security/

Statement by NSC Spokesperson Adrienne Watson on U.S. Cybersecurity Support to Costa Rica | The White House

Source: https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/31/statement-by-nsc-spokesperson-adrienne-watson-on-u-s-cybersecurity-support-to-costa-rica/

Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware | The White House

Source: https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/30/joint-statement-on-efforts-to-counter-the-proliferation-and-misuse-of-commercial-spyware/

Notice on the Continuation of the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities | 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/presidential-actions/2023/03/29/notice-on-the-continuation-of-the-national-emergency-with-respect-to-significant-malicious-cyber-enabled-activities-3/

FACT SHEET: Advancing Technology for Democracy | The White House

Source: https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/29/fact-sheet-advancing-technology-for-democracy-at-home-and-abroad/

Readout of Space Systems Cybersecurity Executive Forum Hosted by the Office of the National Cyber Director and the National Space Council | The White House

Source: https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/28/readout-of-space-systems-cybersecurity-executive-forum-hosted-by-the-office-of-the-national-cyber-director-and-the-national-space-council/

Remarks by President Biden on Investing in America | The White House

Source: https://www.whitehouse.gov/briefing-room/speeches-remarks/2023/03/28/remarks-by-president-biden-on-investing-in-america/

Background Press Call on the President's Executive Order on Commercial Spyware | The White House

Source: https://www.whitehouse.gov/briefing-room/press-briefings/2023/03/27/background-press-call-on-the-presidents-executive-order-on-commercial-spyware/

Executive Order on Prohibition on Use by the United States Government of Commercial Spyware that Poses Risks to National Security | The White House

Source: https://www.whitehouse.gov/briefing-room/presidential-actions/2023/03/27/executive-order-on-prohibition-on-use-by-the-united-states-government-of-commercial-spyware-that-poses-risks-to-national-security/

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.

FACT SHEET: President Biden Signs Executive Order to Prohibit U.S. Government Use of Commercial Spyware that Poses Risks to National Security | The White House

Source: https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/27/fact-sheet-president-biden-signs-executive-order-to-prohibit-u-s-government-use-of-commercial-spyware-that-poses-risks-to-national-security/

Memorandum on Presidential Determination Pursuant to Section 303 of the Defense Production Act of 1950, as amended, on Printed Circuit Boards and Advanced Packaging Production Capability | The White House

Source: https://www.whitehouse.gov/briefing-room/presidential-actions/2023/03/27/memorandum-on-presidential-determination-pursuant-to-section-303-of-the-defense-production-act-of-1950-as-amended-on-printed-circuit-boards-and-advanced-packaging-production-capability/

FACT SHEET: President Biden Announces New Resources to Support Women Small Businesses Owners, Continued Commitment to Supporting America's Entrepreneurs | The White House

Source: https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/27/fact-sheet-president-biden-announces-new-resources-to-support-women-small-businesses-owners-continued-commitment-to-supporting-americas-entrepreneurs/

Memorandum on Presidential Determination Pursuant to Section 303 of the Defense Production Act of 1950, as amended, on Printed Circuit Boards and Advanced Packaging Production Capability | The White House

Source: https://www.whitehouse.gov/briefing-room/presidential-actions/2023/03/27/memorandum-on-presidential-determination-pursuant-to-section-303-of-the-defense-production-act-of-1950-as-amended-on-printed-circuit-boards-and-advanced-packaging-production-capability/

Joint Statement by President Biden and Prime Minister Trudeau | 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/joint-statement-by-president-biden-and-prime-minister-trudeau/

From the Article: "White House. Strengthen Resilience of Critical Mineral and Semiconductor Supply Chains: The United States and Canada will work together to create a strong, environmentally responsible, and resilient North American critical minerals supply chain. "

Articles of Interest

3CX Supply Chain Attack Campaign

Source: https://www.zscaler.com/security-research/3CX-supply-chain-attack-analysis-march-2023

From the Article: "On March 29th 2023, CrowdStrike published a blog outlining a supply chain attack leveraging the 3CXDesktopApp - a softphone application from 3CX. The ThreatLabz Team immediately started hunting for IoCs on the Zscaler Cloud."

Additional sources:
https://www.zscaler.com/security-research/coverage-advisory-3cx-supply-chain-attack-march-2023

https://www.theregister.com/2023/03/30/communications_software_vendor_3cx_hit/

https://www.trendmicro.com/en_us/research/23/c/information-on-attacks-involving-3cx-desktop-app.html

https://www.cybertalk.org/2023/03/31/malicious-supply-chain-attack-hits-3cx-desktop-app/

https://www.tenable.com/blog/3cx-desktop-app-for-windows-and-macos-reportedly-compromised-in-supply-chain-attack

https://www.hackread.com/3cx-desktop-app-supply-chain-attack/

https://www.malwarebytes.com/blog/news/2023/03/3cx-desktop-app-used-in-a-supply-chain-attack

https://heimdalsecurity.com/blog/warning-threat-actors-compromise-3cx-desktop-app-in-a-supply-chain-attack/

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

https://www.darkreading.com/endpoint/automatic-officlal-updates-malicious-3cx-enterprises

https://www.trendmicro.com/en_us/research/23/c/information-on-attacks-involving-3cx-desktop-app.html

https://thehackernews.com/2023/03/3cx-desktop-app-targeted-in-supply.html

https://www.reliaquest.com/blog/3cx-trojan-attack/

https://informationsecuritybuzz.com/supply-chain-attack-hackers-3cx-desktop-app/

https://www.csoonline.com/article/3692250/3cx-desktopapp-compromised-by-supply-chain-attack.html

https://www.bankinfosecurity.com/3cx-desktop-client-under-supply-chain-attack-a-21573

https://unit42.paloaltonetworks.com/3cxdesktopapp-supply-chain-attack/

https://www.sentinelone.com/blog/smoothoperator-ongoing-campaign-trojanizes-3cx-software-in-software-supply-chain-attack/

https://thehackernews.com/2023/03/3cx-supply-chain-attack-heres-what-we.html

https://www.helpnetsecurity.com/2023/03/30/3cx-trojanized-app/

https://www.bankinfosecurity.com/north-korean-lazarus-group-linked-to-3cx-supply-chain-hack-a-21597

https://cyberscoop.com/3cx-supply-chain-attack/

https://cyberintelmag.com/attacks-data-breaches/3cx-acknowledges-supply-chain-attack-as-research-experts-unveil-mac-component/

https://www.securityweek.com/3cx-confirms-supply-chain-attack-as-researchers-uncover-mac-component/

https://securityaffairs.com/144224/hacking/3cx-supply-chain-attack.html

https://nakedsecurity.sophos.com/2023/03/30/supply-chain-blunder-puts-3cx-telephone-app-users-at-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.

https://www.kaspersky.com/blog/supply-chain-attack-on-3cx/47698/

https://www.blackhatethicalhacking.com/news/major-companies-hit-in-ongoing-3cx-voip-supply-chain-attack/

https://www.securityweek.com/malware-hunters-spot-supply-chain-attack-hitting-3cx-desktop-app/

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

https://arstechnica.com/information-technology/2023/03/3cx-knew-its-app-was-flagged-as-malicious-but-took-no-action-for-7-days/

The U.S. Government Restricts the Use of Spyware, White House Says

Source: https://heimdalsecurity.com/blog/the-us-government-restricts-the-use-of-spyware-white-house-says/

From the Article: "At least 50 US government officials are either suspected or confirmed to have been targeted by invasive commercial spyware designed to hack mobile phones, extract data, and track the movements of the victims. "

Additional sources:
https://www.bankinfosecurity.com/us-limits-government-use-advanced-smartphone-spyware-a-21538

https://gizmodo.com/spyware-joe-biden-cybersecurity-nso-group-executive-ord-1850271494

https://thehackernews.com/2023/03/president-biden-signs-executive-order.html

https://www.securityweek.com/us-to-adopt-new-restrictions-on-using-commercial-spyware/

https://www.nextgov.com/cybersecurity/2023/03/biden-admin-targets-misuse-spyware-new-executive-order/384464/

https://cyberscoop.com/white-house-spyware-executive-order/

https://www.csoonline.com/article/3691711/biden-administration-seeks-to-tamp-down-the-spyware-market-with-a-new-ban.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.sentinelone.com/blog/the-good-the-bad-and-the-ugly-in-cybersecurity-week-13-4/

https://www.pandasecurity.com/en/mediacenter/security/federal-agencies-spyware/

https://www.zimperium.com/blog/the-persistent-threat-posed-by-mobile-spyware-to-government-agencies-and-enterprises/

https://www.theregister.com/2023/03/28/biden_spyware_executive_order/

https://informationsecuritybuzz.com/executive-order-limiting-usage-commercial-spyware/

iCloud Keychain Data and Passwords are at Risk From MacStealer Malware

Source: https://www.cysecurity.news/2023/03/icloud-keychain-data-and-passwords-are.html

From the Article: "Uptycs, a cybersecurity company that discovered the information-stealing malware while searching for threats on the dark web, is warning that Mac computers have been the latest targets of updated info-stealing malware."

Additional sources:
https://thehackernews.com/2023/03/new-macstealer-macos-malware-steals.html

https://www.infosecurity-magazine.com/news/macstealer-targets-macos-versions/

https://heimdalsecurity.com/blog/macstealer-macos-malware-steals-passwords-icloud/

https://www.darkreading.com/attacks-breaches/macstealer-malware-plucks-bushels-data-apple-users

https://cyberintelmag.com/malware-viruses/icloud-keychain-passwords-and-data-stolen-by-new-macstealer-macos-malware/

https://www.blackhatethicalhacking.com/news/macstealer-the-new-info-stealing-malware-targeting-mac-users/

https://securityaffairs.com/144099/malware/macstealer-macos-malware.html

https://www.trendmicro.com/en_us/research/23/c/mac-malware-macstealer-spreads-as-fake-p2-e-apps.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.hackread.com/macstealer-malware-macos-catalina-devices/

Cyberwarfare Leaks Reveal Russia's Sweeping Efforts and Potential Targets

Source: https://www.cysecurity.news/2023/04/cyberwarfare-leaks-reveal-russias.html

From the Article: "NTC Vulkan is a cybersecurity consultancy firm based in Moscow, which appears to offer ordinary cybersecurity services on the surface. However, a recent leak of confidential documents has revealed that the company's engineers are also involved in the development of advanced hacking and disinformation tools for the Russian military."

Additional sources:
https://www.theregister.com/2023/03/31/vulkan_files_russia/

https://securityaffairs.com/144340/apt/ntc-vulkan-sandworm-cyberwarfare-arsenal.html

https://www.schneier.com/blog/archives/2023/03/russian-cyberwarfare-documents-leaked.html

https://www.theguardian.com/technology/2023/mar/30/vulkan-files-leak-reveals-putins-global-and-domestic-cyberwarfare-tactics

https://www.darkreading.com/vulnerabilities-threats/vulkan-playbook-leak-exposes-russia-plans-worldwide-cyber-war

https://www.theguardian.com/technology/2023/mar/30/cyberwarfare-leaks-show-russian-army-is-adopting-mindset-of-secret-police

https://www.securityweek.com/leaked-documents-detail-russias-cyberwarfare-tools-including-for-ot-attacks/

APT43: A New Cyberthreat From North Korea

Source: https://heimdalsecurity.com/blog/apt43-a-new-cyberthreat-from-north-korea/

From the Article: "A new North Korean cyber operator has been attributed to a series of attacks conducted to gather strategic intelligence aligned with the state’s geopolitical interests."

Link back to Table of Contents

Additional sources:
https://www.csoonline.com/article/3692288/north-korean-threat-actor-apt43-pivots-back-to-strategic-cyberespionage.html

https://www.securityweek.com/mandiant-catches-another-north-korean-gov-hacker-group/

https://www.theregister.com/2023/03/30/mandian_apt43_north_korea/

https://thehackernews.com/2023/03/north-korean-apt43-group-uses.html

https://www.scmagazine.com/analysis/critical-infrastructure/meet-apt43-the-group-that-hacks-spies-and-steals-for-north-koreas-ruling-elite

https://informationsecuritybuzz.com/north-korean-apt43-finances-spy-activities-cybercrime/

https://industrialcyber.co/ransomware/mandiant-identifies-north-korea-linked-apt43-cyber-operator-using-cybercrime-to-fund-espionage-operations/

14 Million Records Stolen in Data Breach at Latitude Financial Services

Source: https://www.securityweek.com/14-million-records-stolen-in-data-breach-at-latitude-financial-services/

From the Article: "Australian financial services provider Latitude says roughly 14 million user records were stolen in a recent cyberattack."

Additional sources:
https://informationsecuritybuzz.com/customer-details-latitude-financial/

https://www.bankinfosecurity.com/latitude-financial-admits-14m-customer-details-breached-a-21543

https://securityaffairs.com/144137/data-breach/latitude-data-breach-14m-individuals.html

https://www.infosecurity-magazine.com/news/latitude-financial-admits-breach/

https://www.hackread.com/latitude-financial-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.

https://news.hitb.org/content/fears-wider-hacking-theft-latitude-stays-offline

https://heimdalsecurity.com/blog/14-million-customers-latitude-data-breach/

Trojan-Rigged Tor Browser Bundle Drops Malware

Source: https://www.darkreading.com/attacks-breaches/trojan-rigged-tor-browser-bundle-drops-malware

From the Article: "Attackers are targeting cryptocurrency accounts belonging to users in Russia and more than 50 other countries."

Additional sources:
https://thehackernews.com/2023/03/trojanized-tor-browser-installers.html

https://www.infosecurity-magazine.com/news/clipboard-injector-attacks-target/

https://www.hackread.com/fake-tor-browser-installers-clipper-malware/

https://grahamcluley.com/clipboard-injecting-malware-disguises-itself-as-tor-browser-steals-cryptocurrency/

https://cyberintelmag.com/malware-viruses/russians-intended-victims-of-crypto-stealing-malware-that-infects-tor-browsers-with-trojan/

https://www.cysecurity.news/2023/04/trojanized-tor-browser-bundle-drops.html

https://securityaffairs.com/144158/hacking/tor-browser-installers-clipper.html

Russian APT group Winter Vivern targets email portals of NATO and diplomats

Source: https://securityaffairs.com/144263/intelligence/winter-vivern-email-portals-nato.html

From the Article: "A Russian hacking group, tracked Winter Vivern (aka TA473), has been actively exploiting vulnerabilities (CVE-2022-27926) in unpatched Zimbra instances to gain access to the emails of NATO officials, governments, military personnel, and diplomats."

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.theregister.com/2023/03/31/winter_vivern_european_goverments/

https://www.cysecurity.news/2023/04/winter-vivern-hackers-exploit-zimbra.html

https://www.csoonline.com/article/3692249/apt-group-winter-vivern-exploits-zimbra-webmail-flaw-to-target-government-entities.html

https://thehackernews.com/2023/03/winter-vivern-apt-targets-european.html

https://heimdalsecurity.com/blog/nato-and-diplomats-email-portals-targeted-by-russian-apt-winter-vivern/

https://www.cysecurity.news/2023/04/these-apt-hackers-install-malware-by.html

Security breach. Ransomware attack: Sun Pharma says business operations impacted

Source: https://www.thehindubusinessline.com/companies/ransomware-attack-sun-pharma-says-business-operations-impacted/article66667349.ece

From the Article: "Over three weeks after being hit by an information technology (IT) security breach, drugmaker Sun Pharmaceutical Industries said its business operations have been impacted following the incident and efforts to contain and redress the situation."

Additional sources:
https://www.timesnownews.com/technology-science/sun-pharma-hit-by-infamous-ransomware-group-alphv-blackcat-threats-to-release-sensitive-data-article-98998984

https://www.ndtv.com/business/ransomware-attack-to-hurt-revenue-at-sun-pharmaceutical-3896069

https://www.moneycontrol.com/news/business/moneycontrol-research/sun-pharma-ransomware-attack-to-weigh-on-operational-performance-10323331.html

https://www.moneycontrol.com/news/videos/trends/health/cyber-attack-once-again-i-sun-pharma-hit-by-ransomware-10327611.html

https://www.securitynewspaper.com/2023/03/29/fourth-largest-generic-pharmaceutical-company-warns-of-revenue-loss-after-big-ransomware-attack/

https://www.cybersecurityconnect.com.au/commercial/8864-fourth-largest-pharmaceutical-company-in-the-world-admits-to-ransomware-breach

Link back to Table of Contents

Casino Giant Crown Resorts Investigating Ransomware Group's Data Theft Claims

Source: https://www.securityweek.com/casino-giant-crown-resorts-investigating-ransomware-groups-data-theft-claims/

From the Article: "Australian casino giant Crown Resorts says the Cl0p ransomware group contacted them to claim data theft in the GoAnywhere attack."

Additional sources:
https://thewest.com.au/business/crown-resorts-says-ransomware-group-have-illegally-obtained-files-c-10170758

https://www.abc.net.au/news/2023-03-27/crown-resorts-ransomware-threat-by-hackers-data-breach/102151816

https://www.yogonet.com/international//news/2023/03/28/66624-crown-resorts-investigating-potential-data-breach-after-ransomware-group-39s-claims

https://www.bleepingcomputer.com/news/security/crown-resorts-confirms-ransom-demand-after-goanywhere-breach/

https://heimdalsecurity.com/blog/clop-ransomware-exploits-zero-day-vulnerability-data-breach-crown-resorts/

https://securityaffairs.com/144193/data-breach/crown-resorts-clop-ransomware.html

https://www.bleepingcomputer.com/news/security/crown-resorts-confirms-ransom-demand-after-goanywhere-breach/

Parts of Twitter`s Source Code Were Leaked on GitHub, According to Elon Musk

Source: https://heimdalsecurity.com/blog/twitter-source-code-leaked-on-github/

From the Article: "On Friday, March 24th, Twitter sent GitHub a copyright infringement notice, claiming some of the platform`s users leaked parts of their source code. GitHub, the Microsoft-owned service for software developers, reacted promptly and took down the code the same day."

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.bankinfosecurity.com/twitter-says-source-code-leaked-on-github-files-subpoena-a-21536

https://gbhackers.com/twitters-source-code-leaked/

https://www.theguardian.com/technology/2023/mar/27/twitter-legal-source-code-leaked-elon-musk-github

https://www.hackread.com/twitter-source-code-leak-github/

https://www.darkreading.com/attacks-breaches/twitter-source-code-leak-github-potential-cyber-nightmare

https://www.csoonline.com/article/3691776/part-of-twitter-source-code-leaked-on-github.html

New IcedID variants shift from bank fraud to malware delivery

Source: https://www.proofpoint.com/us/newsroom/news/new-icedid-variants-shift-bank-fraud-malware-delivery

From the Article: "New IcedID variants have been found without the usual online banking fraud functionality and instead focus on installing further malware on compromised systems."

Additional sources:
https://www.cysecurity.news/2023/04/icedid-new-era-with-lite-and-fork.html

https://www.scmagazine.com/news/malware/new-icedid-malware-variants-banking-trojans-ransomware

https://informationsecuritybuzz.com/new-icedid-variants-switch-malware-bank-fraud/

https://thehackernews.com/2023/03/icedid-malware-shifts-focus-from.html

https://www.infosecurity-magazine.com/news/variants-icedid-malware-discovered/

https://www.csoonline.com/article/3691897/researchers-warn-of-two-new-variants-of-potent-icedid-malware-loader.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.

Fake DDoS services set up to trap cybercriminals

Source: https://www.malwarebytes.com/blog/news/2023/03/fake-ddos-services-set-up-to-trap-cybercriminals

From the Article: "The “online criminal marketplace” has been disrupted via several fake Distributed Denial of Service (DDoS) tools, according to an announcement from The British National Crime Agency (NCA). "

Additional sources:
https://nakedsecurity.sophos.com/2023/03/28/cops-use-fake-ddos-services-to-take-aim-at-wannabe-cybercriminals/

https://heimdalsecurity.com/blog/the-u-k-police-hunts-cybercriminals-with-fake-ddos-as-a-service-sites/

https://gbhackers.com/fake-ddos-for-hire-websites/

https://www.bitdefender.com/blog/hotforsecurity/uk-police-reveal-they-are-running-fake-ddos-for-hire-sites-to-collect-details-on-cybercriminals/

https://krebsonsecurity.com/2023/03/uk-sets-up-fake-booter-sites-to-muddy-ddos-market/

FDA Announces New Cybersecurity Requirements for Medical Devices

Source: https://www.securityweek.com/fda-announces-new-cybersecurity-requirements-for-medical-devices/

From the Article: "The FDA is asking medical device manufacturers to provide cybersecurity-related information when submitting an application for a new product."

Additional sources:
https://www.darkreading.com/cloud/the-fda-medical-device-cybersecurity-overhaul-real-teeth

https://www.cnn.com/2023/03/29/tech/fda-medical-devices-secured-cyberattacks/index.html

https://www.scmagazine.com/news/device-security/fda-will-refuse-new-medical-devices-for-cybersecurity-reasons-on-oct-1

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

https://www.infosecurity-magazine.com/news/fda-protects-medical-devices-cyber/

https://industrialcyber.co/medical/fda-raises-the-bar-for-cybersecurity-in-medical-devices-requires-premarket-submission-for-cyber-devices/

Ukrainian Cops Bust Phishing Group That Stole $4.3 Million

Source: https://www.bankinfosecurity.com/ukrainian-cops-bust-phishing-group-that-stole-43-million-a-21595

From the Article: "The Ukrainian law enforcement busted a transnational group of scammers that used more than a hundred phishing websites to defraud Europeans. Scammers embezzled nearly $4.4 million by fooling more than a thousand victims to hand over payment card details, say police."

Additional sources:
https://securityaffairs.com/144279/cyber-crime/cyber-police-of-ukraine-cybercrime-gang.html

https://thehackernews.com/2023/03/cyber-police-of-ukraine-busted-phishing.html

https://heimdalsecurity.com/blog/ukrainian-authorities-stop-a-phishing-scam-worth-4-3-million/

https://www.hackread.com/ukraine-busts-phishing-scams-gang/

https://informationsecuritybuzz.com/ukraine-cyberpolice-dismantles-fraud-ring/

Lumen Faces 2 Ransomware Attacks, Working With Experts To Evaluate And Minimize Impact

Source: https://www.benzinga.com/news/23/03/31512889/lumen-faces-2-ransomware-attacks-working-with-experts-to-evaluate-and-minimize-impact

From the Article: "On March 27, 2023, Lumen Technologies, Inc LUMN reported it faced two cybersecurity incidents."

Additional sources:
https://securityaffairs.com/144113/hacking/lumen-suffered-ransomware-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.

https://www.securityweek.com/lumen-technologies-hit-by-two-cyberattacks/

https://www.fiercetelecom.com/telecom/lumen-hit-ransomware-malware-attacks

https://finance.yahoo.com/news/lumen-faces-2-ransomware-attacks-173955639.html

Fortra cyberattack: data on 63,000 children leaks online - Tech Monitor

Source: https://techmonitor.ai/technology/cybersecurity/fortra-cyberattack-ransomware-clop

From the Article: "Data belonging to 63,000 minors has leaked online after a children's mental health provider become the latest victim of an ongoing cyberattack on software company Fortra."

Additional sources:
https://www.cysecurity.news/2023/03/us-healthcare-startup-brightline.html

https://www.bankinfosecurity.com/health-plan-mental-health-provider-stung-by-goanywhere-flaw-a-21550

https://techcrunch.com/2023/03/28/children-data-fortra-ransomware/

Oakland Police Union Threatens To Sue City Over Ransomware Attack

Source: https://sfstandard.com/politics/oakland-police-union-threatens-to-sue-city-over-ransomware-attack/

From the Article: "The attack occurred early last month, and officials with the police union maintain that the city administrator and the mayor have not responded to requests to meet."

Additional sources:
https://www.cbsnews.com/sanfrancisco/news/oakland-ransomware-attack-police-union-threatens-litigation-city-responds/

https://abc7news.com/oakland-ransomware-city-of-hacked-stonewalling-cyberattack/13030898/

Link back to Table of Contents

Hackers Earn Over $1 Million at Pwn2Own Exploit Contest

Source: https://www.securityweek.com/hackers-earn-over-1-million-at-pwn2own-exploit-contest/

From the Article: "Security researchers raked in more than $1 million in prizes at this year's CanSecWest Pwn2Own software exploitation contest."

Additional sources:
https://informationsecuritybuzz.com/pwn2own-hacking-competition-awards-vancouver/

https://gbhackers.com/pwn2own-vancouver/

UK bans TikTok from government mobile phones

Source: https://www.theguardian.com/technology/2023/mar/16/uk-bans-tiktok-from-government-mobile-phones

From the Article: "Britain is to ban the Chinese-owned video-sharing app TikTok from ministers' and civil servants' mobile phones, bringing the UK in line with the US and the European Commission and reflecting deteriorating relations with Beijing."

Additional sources:
https://www.theguardian.com/technology/2023/mar/23/tiktok-to-be-banned-from-uk-parliamentary-devices

https://www.itsecurityguru.org/2023/03/17/tiktok-to-be-banned-from-uk-government-phones/

Modesto hit by apparent Snatch ransomware attack - Audacy

Source: https://www.audacy.com/knxnews/news/national/modesto-ca-hit-by-apparent-snatch-ransomware-attack

From the Article: "After recovering from a cyber attack in February that impacted the city's police department and compromised residents' personal information, Modesto appears to be the target of another ransomware attack."

Additional sources:
https://www.modbee.com/news/local/article273646720.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.scmagazine.com/brief/ransomware/modesto-ransomware-attack-claimed-by-snatch-cybercrime-operation

Ransomware Actors May Be Targeting Organizations With Cyber Insurance

Source: https://mytechdecisions.com/network-security/ransomware-actors-may-be-targeting-organizations-with-cyber-insurance/

From the Article: "Cybersecurity insurance is becoming a popular option for organizations looking to protect themselves from the financial risks of a cyberattack, but new data shows that organizations with cyber insurance may be more appealing to ransomware attackers."

Additional sources:
https://www.jdsupra.com/legalnews/the-dangers-of-dialogue-ransomware-9807050/

2 Reshoring and FDI Up a Record 53%

Source: https://www.industrialheating.com/articles/97524-reshoring-and-fdi-up-a-record-53

From the Article: "According to the Reshoring Initiative's 2022 data report, reshoring and foreign direct investment (FDI) job announcements in 2022 were at the highest rate ever recorded. There was 364,000 reshoring and FDI jobs announced for 2022, which was up 53% from 2021's record number. Fourth-quarter announcements accelerated even more than anticipated due to the Chips and Infrastructure Acts and deglobalization trends."

Additional sources:
https://www.automation.com/en-us/articles/march-2023/reshoring-fdi-up-53-percent-new-record

ChatGPT Vulnerability May Have Exposed Users' Payment Information

Source: https://www.infosecurity-magazine.com/news/chatgpt-vulnerability-payment/

From the Article: "The breach was caused by a bug in an open-source library."

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://latesthackingnews.com/2023/03/29/chatgpt-vulnerability-exposed-users-convos-and-payment-details/

TSA cybersecurity amendment for airport, aircraft operators pushes for cyber design engineering evolution

Source: https://industrialcyber.co/features/tsa-cybersecurity-amendment-for-airport-aircraft-operators-pushes-for-cyber-design-engineering-evolution/

From the Article: "Responding to persistent cybersecurity threats against critical U.S. infrastructure, the Transportation Security Administration (TSA) division issued in March an emergency cybersecurity amendment to the security programs of certain TSA-regulated airport and aircraft operators."

Additional sources:
https://www.sentinelone.com/blog/meeting-the-tsa-cybersecurity-requirements-for-airports-and-aircraft-with-sentinelone-singularity-xdr/

White House announces $25 million in cybersecurity aid to Costa Rica | CyberScoop

Source: https://cyberscoop.com/white-house-announces-25-million-in-cybersecurity-aid-to-costa-rica/

From the Article: "The U.S. government will provide Costa Rica with $25 million in assistance to bolster its cybersecurity efforts, a senior administration official said Wednesday, nearly a year after the country suffered a series of devastating ransomware attacks at the hands of a Russian-linked cybercrime group."

Additional sources:
https://therecord.media/biden-administration-commits-25-million-costa-rica-ransomware-recovery

Hey, Siri: Hackers Can Control Smart Devices Using Inaudible Sounds

Source: https://www.darkreading.com/vulnerabilities-threats/siri-hackers-control-smart-devices-inaudible-sounds

From the Article: "A technique, dubbed the "Near-Ultrasound Inaudible Trojan" (NUIT),

allows an attacker to exploit smartphones and smart speakers over the Internet, using sounds undetectable by humans."

Additional sources:
https://www.malwarebytes.com/blog/news/2023/03/smart-home-assistants-at-risk-from-nuit-ultrasound-attack

Florida city water cyber incident allegedly caused by employee error

Source: https://gcn.com/cybersecurity/2023/03/florida-city-water-cyber-incident-allegedly-caused-employee-error/384267/

Summary: Further details on the Oldsmar water incident indicate that instead of a cyber-attack, as was initially reported, it was user error. Organization procedures were used to correct and further educate the user about the error.

Additional sources: http://scadamag.infracritical.com/index.php/2023/03/29/florida-city-water-cyber-incident-allegedly-caused-by-employee-error/

Taking Japan–Australia defense cooperation to the next level | The Strategist

Source: https://www.aspistrategist.org.au/taking-japan-australia-defence-cooperation-to-the-next-level/

From the Article: "After decades of gradual military build-up by China, territorial disputes with China and Russia, and increasing concern about North Korea's missile-strike capability, Japan is once again reinventing itself and rapidly moving from the pacifist stance it has embraced since the end of World War II."

10-year-old Windows bug with 'opt-in' fix exploited in 3CX attack

Source: https://www.bleepingcomputer.com/news/microsoft/10-year-old-windows-bug-with-opt-in-fix-exploited-in-3cx-attack/

Summary: The exploit is an opt-in patch dating from 2013: from the article: "On December 10, 2013, Microsoft released an update for all supported releases of Microsoft Windows that changes how signatures are verified for binaries signed with the Windows Authenticode signature format," explains Microsoft's disclosure for the CVE-

2013-3900. "This change can be enabled on an opt-in basis."

Supply Chain Attacks: 'The Best Bang For Your Buck'

Source: https://duo.com/decipher/supply-chain-attacks-the-best-bang-for-your-buck

From the article: "Researchers have connected the attack to a group that CrowdStrike calls Labyrinth Chollima, which overlaps with the Lazarus Group, a high-line attack team associated with the North Korean government. The attackers were able to compromise the update mechanism for the 3CX Windows and macOS apps and then push malicious code. Only the desktop apps are affected, not the web version."

Critical infrastructure gear is full of flaws, but hey, at least it's certified - The Register

Source: https://www.theregister.com/2023/03/23/critical_infrastructure_hardware_flaws/

Summary: Upcoming academic paper analyzes OT product for security vulnerabilities. Worse, many of the products claim 62443 certification, but appear to have weak implementation.

OMB Approves DOD DIB Cybersecurity NPRM

Source: https://chemical-facility-security-news.blogspot.com/2023/03/omb-approves-dod-dib-cybersecurity-nprm.html

From the article: "Participation in the voluntary DIB CS Program enables DoD contractors to access Government Furnished Information and collaborate with the DoD Cyber Crime Center (DC3) to better respond to and mitigate cyber threats. In order to join the DIB CS Program, there is an initial labor burden to apply to the program and provide point of contact information which is estimated to take 20 minutes per company."

When will I be able to verify an SBOM? Probably never.

Source: http://tomalrichblog.blogspot.com/2023/03/when-will-i-be-able-to-verify-sbom.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.

Summary: Analysis of why it might be hard for SBOM verification from a software suppliers. There is movement to mitigate this behavior, however, it will take process and failures to identify points to fix.

Covert Channel Between the CPU and An FPGA By Modulating The Usage of the Power Distribution Network

Source: https://semiengineering.com/covert-channel-between-the-cpu-and-an-fpga-by-modulating-the-usage-of-the-power-distribution-network/

Summary: technique on SOC-FPGA covert channels, can be used to discover secrets

The life and times of sysinternals how one developer changed the face of malware analysis

Source: https://www.sentinelone.com/labs/the-life-and-times-of-sysinternals-how-one-developer-changed-the-face-of-malware-analysis/

Summary: Embedded video has Mark Russinovich go through the history of SysInternals, a tool used for debugging and profiling systems.

Fighting Security Entropy

Source: https://www.philvenables.com/post/fighting-security-entropy

Summary: Phil Venables has an article about using control reliability engineering to continuously monitor effectiveness of security controls (as the control effectiveness degrades over the life of a product)

Pause Giant AI Experiments: An Open Letter - Future of Life Institute

Source: https://futureoflife.org/open-letter/pause-giant-ai-experiments/

Summary: An open letter asking OpenAI to pause development of AI engines more powerful than ChatGPT-4, or have the Biden Administration step in an forceibly enact a moratorium.

Link back to Table of Contents

ReTrustFSM: Toward RTL Hardware Obfuscation-A Hybrid FSM Approach

Source: https://ieeexplore.ieee.org/document/10043856

Summary: Supply chain resilient technique for integrated circuits.

TSMC's 4/5nm Chips Generate Higher Revenue than 6/7nm

Source: https://abachy.com/news/tsmcs-45nm-chips-generate-higher-revenue-67nm

From the Article: "TSMC's 4nm and 5nm products brought in about $19.4 billion last year, and this year the company's core revenue could grow by $3.6 billion. To some extent, this will compensate for the decline in sales revenue. Both 7-nm and 6-nm products, as well as to keep the company's total revenue for the year approximately at the level of the previous year ($76 billion)."

Ukraine scrambles to draft cyber law, legalizing its volunteer hacker army

Source: https://www.newsweek.com/ukraine-drafting-new-law-legalizing-volunteer-hacker-cyber-army-red-cross-1786814

From the Article: "Ukraine's government is drafting a new law to bring its volunteer hacker brigade, the IT Army, into the armed forces, aiming to put an end to uncertainty about its status in a legal gray area that has drawn pointed warnings from the Red Cross."

The Biden-Harris Administration Releases New National Cybersecurity Strategy

Source: https://www.lawfareblog.com/biden-harris-administration-releases-new-national-cybersecurity-strategy

From the Article: "President Joe Biden walks with Vice President Kamala Harris and Secretary of Defense Lloyd Austin. (White House Photo by Adam Schultz) On March 2, the Biden administration released its long-awaited National Cybersecurity Strategy. The new strategy comes more than two years after President Biden took office and more than four years after the Trump administration issued its National Cyber Strategy in September 2018."

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 Biden Administration's National Cybersecurity Strategy Calls for a Shift Toward More Cybersecurity Regulation | Morrison Foerster

Source: https://www.mofo.com/resources/insights/230306-the-biden-administrations-national-cybersecurity-strategy

From the Article: "The strategy: Seeks for the first time to shift liability onto developers of insecure software products and services for developing insecure products; Calls on Congress to enact national legislation to place limits on the ability to collect, use, transfer, and maintain personal data; Calls for cybersecurity minimum standards and other regulations to secure critical infrastructure sectors; and Seeks to leverage federal procurement rules to impose cybersecurity requirements, with a threat of civil actions against government grantees and contractors that fail to meet cybersecurity obligations. "

UK boosts quantum tech with £2.5bn 10 year plan

Source: https://www.eenewseurope.com/en/uk-boosts-quantum-tech-with-2-5bn-10-year-plan/

From the Article: "The UK government has launched a ten year plan for quantum technology with a doubling of funding to £2.5bn (€2.85bn). It aims to almost double its market share in quantum sensing, timing and networking as well as computing."

Use of IPFS in mass and targeted phishing campaigns

Source: https://securelist.com/ipfs-phishing/109158/

From the Article: "Unfortunately, the "new internet" will still remain a playground for criminals who will employ cutting-edge technologies for their old sport of data theft, financial machinations and the like. In this article, I will dwell on how they use one of the WEB 3.0 technologies — the distributed file system IPFS — for email phishing attacks."

How will Wolfspeed's expansion into Europe impact the region's stronghold in SiC devices?

Source: https://www.yolegroup.com/press-release/how-will-wolfspeeds-expansion-into-europe-impact-the-regions-stronghold-in-sic-devices/

Link back to Table of Contents

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

From the Article: "On 1 February, Wolfspeed and ZF announced a strategic partnership to target future silicon carbide semiconductor systems and devices for mobility, industrial and energy applications. One way it will achieve this is by building significant SiC production capacity in Europe. Wolfspeed's new facility in Germany will be the world's largest 8-inch dedicated SiC device fab, and the only fab in Europe capable of producing 8-inch SiC wafers at high volume (excluding some SiC-compatible capacity at STMicroelectronics)."

U.S. Prepares to Establish Its $11 Billion NSTC - EE Times

Source: https://www.eetimes.com/u-s-prepares-to-establish-11-billion-nstc/

From the Article: "The effort is likened to the collaborative endeavor that created the world's first nuclear weapons. To take innovation from lab to fab, the NSTC, which is part of the U.S. CHIPS Act, will be a public-private consortium joining government and industry, as well as academia, entrepreneurs, workforce representatives and investors."

The US has gotten the day to day right in Africa policy. Time to think bigger.

Source: https://www.atlanticcouncil.org/blogs/africasource/the-us-has-gotten-the-day-to-day-right-in-africa-policy-time-to-think-bigger/

From the Article: "The summit also gave additional momentum to US efforts to support digitization in African markets. While hugely important and widely supported across the US-Africa policy community, Biden's new flagship Africa initiative—Digital Transformation with Africa—simply builds on old programs such as the US International Development Finance Corporation's Connect Africa and the US Trade and Development Agency's Access Africa (among others with overlapping mandates)."

South Korean chip giants dodge 'worst-case scenario' in new US proposal

Source: https://www.scmp.com/week-asia/politics/article/3214817/tech-war-relief-south-korean-semiconductor-giants-dodge-worst-case-scenario-us-proposal-chip-output

From the Article: "Korean chip makers avoided having to stop all production expansion, innovation in China, under new proposed rules by the US, say analysts The US wants to ban recipients of its Chips and Science Act from expanding chip production in China or other 'countries of concern' by more than 5 per cent for next 10 years"

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.

Canada and US forge stronger ties against 'disruptive' China

Source: https://www.scmp.com/news/world/united-states-canada/article/3214812/biden-and-trudeau-pledge-stand-together-against-authoritarian-regimes

From the Article: "North American leaders push for stronger joint supply chains and less dependence on other countries for critical minerals and semiconductors Canadians Michael Spavor and Michael Kovrig, who China had detained for more than 1,000 days until 2021, attend the speeches"

China's top memory chip maker YMTC sees improved global market demand in 2023

Source: https://www.scmp.com/tech/big-tech/article/3214773/tech-war-us-blacklisted-ymtc-chinas-top-memory-chip-maker-sees-improved-global-market-demand-2023

From the Article: "Yangtze Memory Technologies Co sees boost in global demand for NAND Flash products from makers of smartphones, servers and personal computers YMTC's chief operating officer said the firm continues to push for innovation, business diversification and talent development, despite US sanctions"

Biden administration moves to stop China, Russia from using US chips funding

Source: https://www.scmp.com/news/world/united-states-canada/article/3214362/biden-administration-moves-stop-china-and-russia-using-us-chips-funding

From the Article: "The Commerce Department's proposed guidelines say firms can't use the funds for projects outside the US or to build facilities in 'foreign entities of concern' There are also plans to restrict joint research or tech licensing for certain types of semiconductors deemed 'critical to national security'"

'China won't just swallow this': Beijing envoy warns Dutch over chip curbs

Source: https://www.scmp.com/news/china/article/3214361/china-wont-just-swallow-beijing-envoy-warns-dutch-retaliation-chip-curbs

From the Article: "Tan Jian, Chinese ambassador to the Netherlands, says export restrictions on chip technology 'will not be without consequences' The Dutch firm ASML is the world's leading producer of photolithography machines crucial to making advanced microchips"

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

China's flagship CPU designer puts on a brave face amid US sanctions

Source: https://www.scmp.com/tech/tech-war/article/3213889/tech-war-chinas-flagship-cpu-designer-loongson-puts-brave-face-amid-us-sanctions

From the Article: "Loongson said it is evaluating the advanced 7-nm process from a number of foundries to manufacture its future chips, which include GPUs The company launched its home-grown 3A5000 CPU at the end of 2020, which was made on a now-restricted process node of 14-nm"

Ask nvidia ceo gtc gpu shortage looming

Source: https://www.fierceelectronics.com/electronics/ask-nvidia-ceo-gtc-gpu-shortage-looming

From the Article: "A question likely to come up for CEO Jensen Huang at Nvidia's global AI GTC conference starting Monday is how well his company is keeping up with semiconductor demand—mainly GPUs-- for training and inference functions used in a cascade of applications, especially to sate the seemingly endless appetite for chatbots like Open.AI's Chat GPT4."

China crisis is a TikToking time bomb

Source: https://www.theregister.com/2023/03/27/china_crisis_is_a_tiktoking/

From the Article: "OPINION As country after country bans TikTok from official systems, it's fair to ask what's so dodgy about a social network filled with dance crazes, makeup advice and cats. You can understand why selling the Middle Kingdom state-of-the-art EUV lithography gear might be a bad idea, but this? Is it the xenophobia China often blames for Western reticence? Plain old trade barriers? Cold war cultural imperialism? No, it really is a security matter, and one that's far more serious than it looks."

NATO preps tech competition to solve real-world security issues

Source: https://www.defensenews.com/global/europe/2023/03/24/nato-preps-tech-competition-to-solve-real-world-security-issues/

From the Article: "STUTTGART, Germany — NATO's nascent defense technology accelerator is preparing to launch the first several competition-style programs, meant to help the alliance find solutions to emerging technology problems."

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.

2026 all time high in store for global 300mm semiconductor capacity after 2023 slowdown semi reports

Source: https://www.semi.org/en/news-media-press-releases/semi-press-releases/2026-all-time-high-in-store-for-global-300mm-semiconductor-capacity-after-2023-slowdown-semi-reports

From the Article: "MILPITAS, Calif. — March 27, 2023 — Semiconductor manufacturers worldwide are forecast to increase 300mm fab capacity to an all-time high of 9.6 million wafers per month (wpm) in 2026, SEMI announced today in its 300mm Fab Outlook to 2026 report. After strong growth in 2021 and 2022, the 300mm capacity expansion is expected to slow this year due to soft demand for memory and logic devices."

How often should security audits be?

Source: https://cybersecurity.att.com/blogs/security-essentials/how-often-should-security-audits-be

From the Article: "In today's digital world, it's no surprise that cyberattacks are becoming more frequent and intense. Enterprises worldwide are trying to defend themselves against attacks such as ransomware, phishing, distributed denial of service and more."

Now Patched Outlook Zero Day Gains PoC And Growing Concerns

Source: https://www.scmagazine.com/news/email-security/outlook-zero-day-poc-concerns

From the Article: "Security teams are sounding an alarm about a critical zero-day bug Microsoft patched earlier this month that allows adversaries to trigger an elevation of privilege attack within all versions of Microsoft's Windows Outlook. They fear a recently released proof-of-concept attack coupled with the ease of exploitation of the flaw could lead to "broad, rapid adoption" of the vulnerability."

Binary error: How and why governments need a cyber security rethink

Source: https://www.lowyinstitute.org/the-interpreter/binary-error-how-why-governments-need-cyber-security-rethink

From the Article: "Deterrence of hostile states in cyberspace misses the point when operations concentrate on only "offence" vs "defence"."

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 Uncovers Evidence of Russian Hackers Exploiting Outlook Vulnerability

Source: https://www.blackhatethicalhacking.com/news/microsoft-uncovers-evidence-of-russian-hackers-exploiting-outlook-vulnerability/

From the Article: "Microsoft has issued guidance to help its customers detect the indicators of compromise (IoCs) associated with a recently fixed Outlook vulnerability. The critical flaw, tracked as CVE-2023-23397, allowed attackers to carry out privilege escalation, enabling them to steal NT Lan Manager (NTLM) hashes and stage a relay attack without any user interaction. "

Rhadamanthys: The "Everything Bagel" Infostealer

Source: https://research.checkpoint.com/2023/rhadamanthys-the-everything-bagel-infostealer/

From the Article: "We present a method of forensically resolving API calls of homebrew function tables in "orphaned" memory dumps from concluded sandbox runs, using the in-memory addresses alone."

27th March – Threat Intelligence Report

Source: https://research.checkpoint.com/2023/27th-march-threat-intelligence-report/

From the Article: "New victims of Clop ransomware gang that leveraged for the attack purpose a zero-day security flaw (CVE-2023-0669) in the Fortra GoAnywhere Managed File Transfer system were disclosed."

BrandPost: The convergence of IT and OT and its impact on growing infrastructure risks

Source: https://www.csoonline.com/article/3691618/the-convergence-of-it-and-ot-and-its-impact-on-growing-infrastructure-risks.html

From the Article: "Internet-of-Things (IoT) and Operational Technology (OT) devices represent a rapidly expanding, often unchecked risk surface that is largely driven by the technology's pervasiveness, vulnerability, and cloud connectivity."

BrandPost: Public-Private Partnerships are Essential to Strengthen Cybersecurity Globally

Source: https://www.csoonline.com/article/3691813/public-private-partnerships-are-

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.

essential-to-strengthen-cybersecurity-globally.html#tk.rss_all

From the Article: "Cyberattacks are on the rise, and so are the chances that your organization will fall victim to a breach. More than 84% of organizations experienced at least one cyberattack last year. "

Updates from the MaaS: new threats delivered through NullMixer

Source: https://securityaffairs.com/144092/malware/maas-threats-delivered-through-nullmixer-malware.html

From the Article: "A technical analysis of NullMixer malware operation revealed Italy and France are the favorite European countries from the attackers' perspective."

Rogue ChatGPT extension FakeGPT hijacked Facebook accounts

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

From the Article: "A tainted version of the legitimate ChatGPT extension for Chrome, designed to steal Facebook accounts, has thousands of downloads."

Emotet Malware Spread as Counterfeit IRS W-9 Tax Forms

Source: https://cyberintelmag.com/malware-viruses/emotet-malware-spread-as-counterfeit-irs-w-9-tax-forms/

From the Article: "A novel Emotet phishing attack pretends to be W-9 tax forms delivered by employers and the Internal Revenue Service to target American taxpayers. A well-known malware outbreak called Emotet was previously delivered by phishing emails that included Microsoft Word and Excel documents with malicious macros that installed the malware. "

Dependence on Chinese-made tech threatens grid, experts warn

Source: https://cyberscoop.com/chinese-grid-equipment-us-grid/

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

From the Article: "The largely unknown amount of Chinese-made equipment within the North American grid is a threat to national security, experts warned during a Thursday congressional hearing that explored cybersecurity vulnerabilities within the electric sector."

Fact or fiction, hacktivists' claims of industrial sabotage in Russia or Ukraine get attention online

Source: https://cyberscoop.com/hacktivist-target-operational-technology/

From the Article: "Hacktivist groups on both sides of the Ukraine war increasingly claim to have infiltrated critical infrastructure networks in a bid to stoke fears about their abilities to disrupt sensitive operations, the cybersecurity firm Mandiant said in a report released Wednesday."

FCC rules aims to curb scourge of robotexts assaulting Americans' phones

Source: https://cyberscoop.com/fcc-robotext-scam-phishing-robocall/

From the Article: "The Federal Communications Commission on Thursday adopted its first rules to tackle a growing scourge of scam text messages, a move that resembles the agency's crackdown that helped reduce the number of unwanted robocalls."

How artificial intelligence is revolutionizing cyber security

Source: https://www.cybertalk.org/2023/03/27/how-artificial-intelligence-is-revolutionizing-cyber-security/

From the Article: "In recent years, artificial intelligence (AI) has become one of the most sure-fire and strategic tools available for cyber security professionals. Due to the increasing sophistication of cyber attacks, cyber security experts have broadly turned to AI in order to enhance abilities to detect and prevent cyber threats."

GoAnywhere Hack Targets UK Pension Protection Fund

Source: https://www.cysecurity.news/2023/03/goanywhere-hack-targets-uk-pension.html

Link back to Table of Contents

From the Article: "Among the largest asset managers in the United Kingdom, the U.K. Pension Protection Fund, which manages £39 billion in assets, confirmed that the hack against GoAnywhere, the popular file-transferring service, had impacted it."

Watch Out for These Common Signs to Identify an Email Phishing Scam

Source: https://www.cysecurity.news/2023/03/watch-out-for-these-common-signs-to.html

From the Article: "Cybercriminals most frequently use phishing as a method of attack. This communication is a hoax designed to trick the recipient into disclosing private information, sending money, or clicking on a dangerous link. Usually, it is transmitted by email, social media direct messages, or some other text-based method. "

Malvertising Gives Cybercriminals Access to Big Technologies

Source: https://www.cysecurity.news/2023/03/malvertising-gives-cybercriminals.html

From the Article: "Malvertising has been a more popular tool employed by cybercriminals in recent years to exploit unsuspecting internet users. When people click on an infected ad, malware is transferred to their computers and mobile devices, which is known as malvertising."

A ChatGPT Bug Exposes Sensitive User Data

Source: https://www.cysecurity.news/2023/03/a-chatgpt-bug-exposes-sensitive-user.html

From the Article: "OpenAI's ChatGPT, an artificial intelligence (AI) language model that can produce text that resembles human speech, has a security flaw. The flaw enabled the model to unintentionally expose private user information, endangering the privacy of several users. This event serves as a reminder of the value of cybersecurity and the necessity for businesses to protect customer data in a proactive manner."

Cybersecurity vs. Everyone: From Conflict to Collaboration

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/operations/cybersecurity-vs-everyone-from-conflict-to-collaboration

From the Article: "Don't assume stakeholders outside security understand your goals and priorities, but consider how you'll communicate with them to gain their support."

BBC urges staff to delete TikTok from company mobile phones

Source: https://www.theguardian.com/technology/2023/mar/19/bbc-urges-staff-to-delete-tiktok-from-company-mobile-phones

From the Article: "The BBC has urged its staff to delete the Chinese-own social media app TikTok from corporate mobile phones."

Supply Chain Attack via New Malicious Python Packages

Source: https://www.fortinet.com/blog/threat-research/supply-chain-attack-via-new-malicious-python-packages

From the Article: "FortiGuard Labs team recently discovered over 60 zero-day attacks embedded in PyPI packages between early February and mid-March of 2023."

ChatGPT Exposes Email Address of Other Users – Open-Source Bug

Source: https://gbhackers.com/chatgpt-exposes-email-address/

From the Article: "There were a number of users whose email addresses were exposed accidentally by ChatGPT's website recently. While OpenAI asserted that the cause was a bug in the Redis client open-source library. "

Hackers Exploited Critical Microsoft Outlook Vulnerability To Gain Exchange Server Access

Source: https://gbhackers.com/microsoft-outlook-vulnerability/

From the Article: "In response to a recent vulnerability identified in Outlook, Microsoft recently published a proper guide for its customers to help them discover the associated

IoCs."

CISA to Start Issuing Early-Stage Ransomware Alerts

Source: https://www.hackread.com/cisa-early-stage-ransomware-alerts/

From the Article: "According to CISA, this new initiative will be helpful for organizations/institutions in the public health, education, and government sectors."

Journalist Targeted in USB Drive Bombing Attack

Source: https://www.hackread.com/journalist-targeted-usb-drive-bombing-attack/

From the Article: "According to the attorney general of Ecuador, a terrorism investigation has been launched after the incident took place in the country."

Avoiding the Pitfalls of Tax Season: Philadelphia Warns Against Sophisticated Phishing Attacks

Source: https://heimdalsecurity.com/blog/philadelphia-warns-against-sophisticated-phishing-attacks/

From the Article: "According to the city of Philadelphia, cybersecurity recommendations have been issued in response to an Internal Revenue Service (IRS) warning against tax-based phishing attempts. "

Enhanced Version of the BlackGuard Stealer Spotted in the Wild

Source: https://heimdalsecurity.com/blog/enhanced-version-of-the-blackguard-stealer-spotted-in-the-wild/

From the Article: "A new variant of the BlackGuard stealer has been discovered in the wild, with new features such as USB propagation, persistence mechanisms, the ability to inject more payloads into memory, and the ability to target more crypto wallets."

Link back to Table of Contents

VERT Reads All About It - Cybersecurity News March 27, 2023

Source: https://www.tripwire.com/state-of-security/vert-reads-all-about-it-cybersecurity-news-march-27-2023

From the Article: "The Tripwire Vulnerability Exposure and Research Team (VERT) keeps its finger on the cybersecurity pulse. Check out some of the stories that stood out for us recently: WordPress forced the patching of WooCommerce Plugin The WooCommerce Plugin is subject to a privilege escalation vulnerability where an unauthenticated attacker could gain admin access to vulnerable stores."

FBI warns of criminal hackers using BEC tactics to facilitate acquisition of commodities, defrauding vendors

Source: https://industrialcyber.co/threat-landscape/fbi-warns-of-criminal-hackers-using-bec-tactics-to-facilitate-acquisition-of-commodities-defrauding-vendors/

From the Article: "The Federal Bureau of Investigation (FBI) issued a public service announcement warning the public of criminal hackers using Business Email Compromise (BEC) schemes to facilitate the acquisition of commodities and defrauding vendors."

Dragos' Lee calls upon CISA to enforce cybersecurity requirements, as industrial cyber threat landscape shifts irreversibly

Source: https://industrialcyber.co/industrial-cyber-attacks/dragos-lee-calls-upon-cisa-to-enforce-cybersecurity-requirements-as-industrial-cyber-threat-landscape-shifts-irreversibly/

From the Article: "Prioritizing OT/ICS networks is required, with an emphasis on security measures that have proven effective against attackers and going beyond just identifying and adopting best practices used in other domains like business information technology (IT), Robert M. Lee, CEO and co-founder of industrial cybersecurity company Dragos informed the U.S. Senate Committee on Energy and Natural Resources."

Microsoft Fixes Security Flaw in Windows Screenshot Tools

Source: https://www.infosecurity-magazine.com/news/microsoft-fixes-flaw-windows/

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: "Information disclosure vulnerability aCropalypse could enable malicious actors to recover sections of screenshots."

Nominations are Open for 2023's European Cybersecurity Blogger Awards

Source: https://www.itsecurityguru.org/2023/03/20/nominations-are-open-for-2023s-european-cybersecurity-blogger-awards/

From the Article: "If you can believe it, it's been a decade since the annual European Cybersecurity Blogger Awards initially launched in 2013! That's ten years of celebrating the bloggers, vloggers, podcasters and social media influencers who have played a fundamental role in shaping the cybersecurity community as well as educating the wider public."

baserCMS vulnerable to arbitrary file uploads

Source: https://jvn.jp/en/jp/JVN61105618/

From the Article: "baserCMS provided by baserCMS Users Community allows an authenticated user to upload arbitrary files."

Cyber Insurers Quietly Remove Coverage for Social Engineering and Fraudulent Instruction Claims

Source: https://blog.knowbe4.com/cyber-insurers-remove-social-engineering-coverage

From the Article: "As cyber insurers become more experienced in what kinds of claims are being presented, and the threat action details therein, specific types of coverages are no longer being included."

Critical Vulnerability Fixed In WooCommerce Payments WordPress Plugin

Source: https://latesthackingnews.com/2023/03/27/critical-vulnerability-fixed-in-woocommerce-payments-wordpress-plugin/

From the Article: "Security researcher Michael Mazzolini of GoldNetwork caught an authentication bypass vulnerability in the WooCommerce Payments WordPress plugin."

Link back to Table of Contents

Study Reveals Inaudible Sound Attack Threatens Voice Assistants

Source: https://latesthackingnews.com/2023/03/27/study-reveals-inaudible-sound-attack-threatens-voice-assistants/

From the Article: "A recent study reveals how attackers can trigger vulnerabilities in voice assistants for malicious purposes."

Android App From China Executed Zero Day Exploit On Millions Of Devices

Source: https://arstechnica.com/information-technology/2023/03/android-app-from-china-executed-0-day-exploit-on-millions-of-devices/

From the Article: "Android apps digitally signed by China's third-biggest e-commerce company exploited a zero-day vulnerability that allowed them to surreptitiously take control of millions of end-user devices to steal personal data and install malicious apps, researchers from security firm Lookout have confirmed."

Ransomware gunning for transport sector's OT systems next

Source: https://www.malwarebytes.com/blog/news/2023/03/ransomware-gunning-for-transport-sectors-ot-systems-next

From the Article: "ENISA (the European Union Agency for Cybersecurity) has reason to believe that ransomware gangs will begin targeting transportation operational technology (OT) systems in the foreseeable future."

Food giant Dole reveals more about ransomware attack

Source: https://www.malwarebytes.com/blog/news/2023/03/food-giant-dole-reveals-more-about-ransomware-attack

From the Article: "Fruit and vegetable producer Dole has confirmed attackers behind its February ransomware attack accessed employee data. The company hasn't revealed the number of staff impacted."

Link back to Table of Contents

Pro-Russian Hacktivists: A Reaction to a Western Response to a Russian Aggression

Source: https://blog.radware.com/security/2023/03/pro-russian-hacktivists-western-response-to-russian-aggression/

From the Article: "Newton's third law of motion states that for every action, there is an equal and opposite reaction. With a slight alteration, Newton's law can be applied to geopolitics: for every action, there will be a more extensive opposite reaction."

How scammers employ IPFS for email phishing

Source: https://securelist.com/ipfs-phishing/109158/

From the Article: "The idea of creating Web 3.0 has been around since the end of 2000s. The new version of the world wide web should repair the weak points of Web 2.0., some of which are: featureless content, prevalence of proprietary solutions, and lack of safety in a centralized user data storage environment, where a massive leak is likely should just one server be compromised. "

Updates from the MaaS: new threats delivered through NullMixer

Source: https://securityaffairs.com/144092/malware/maas-threats-delivered-through-nullmixer-malware.html

From the Article: "A technical analysis of NullMixer malware operation revealed Italy and France are the favorite European countries from the attackers' perspective."

Malicious Python Package uses Unicode support to evade detection

Source: https://securityaffairs.com/144070/malware/malicious-python-package-uses-unicode.html

From the Article: "Supply chain security firm Phylum discovered a malicious Python package on the Python Package Index (PyPI) repository that uses Unicode to evade detection and deliver information-stealing 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.

The Role of Human Resources in Cybersecurity

Source: https://securityintelligence.com/articles/role-human-resources-cybersecurity/

From the Article: "The human resources (HR) department is an integral part of an organization. They work with all departments with a wider reach than even IT. As a highly visible department, HR can support and improve an organization's security posture through employee training."

GoAnywhere Zero-Day Attack Hits Major Orgs

Source: https://www.securityweek.com/goanywhere-zero-day-attack-hits-major-orgs/

From the Article: "Several major organizations are confirming impact from the latest zero-day exploits hitting Fortra's GoAnywhere software."

Microsoft releases security update for Snipping tool flaw

Source: https://www.2-spyware.com/microsoft-releases-security-update-for-snipping-tool-flaw

From the Article: "Snipping tool flaw puts Windows users at risk Users can screenshot a section of their computer screen and save it as an image file using Windows' built-in Snipping Tool. "

EPA Issues Cybersecurity Regulations for Public Water Systems: How Tenable Can Help

Source: https://www.tenable.com/blog/epa-issues-cybersecurity-regulations-for-public-water-systems-how-tenable-can-help

From the Article: "The U.S. Environmental Protection Agency (EPA) issued a memorandum on March 3, 2023, directing states to include cybersecurity assessments when they conduct sanitation surveys, or audits, of public water systems (PWSs)."

Tenable Cyber Watch: U.K. Cyber Agency Raises Privacy Concerns About ChatGPT, CISA Program Tackles Ransomware in Critical Infrastructure, and more

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.tenable.com/blog/tenable-cyber-watch-u-k-cyber-agency-raises-privacy-concerns-about-chatgpt-cisa-program

From the Article: "This week's edition of the Tenable Cyber Watch unpacks CISA's new pilot program that detects vulnerabilities in critical infrastructure and addresses the FBI's plea for more ransomware victims to report attacks."

Defense Production Act Title III Presidential Determination for Printed Circuit Boards and

Source: https://www.defense.gov/News/Releases/Release/Article/3342032/defense-production-act-title-iii-presidential-determination-for-printed-circuit/

From the Article: "President Joe Biden signed a presidential determination (PD) authorizing the use of Defense Production Act to support the nation's domestic Printed Circuit Boards (PrCB) and Advanced Packaging industrial base. The PD allows the Department of Defense (DoD) to utilize its Defense Production Act (DPA) Title III authorities to invest in advanced microelectronics capacity and ensure the production of state-of-the-art integrated circuits in the United States."

Pentagon CIO places high priority on developing GPS alternatives with growing threat of great power conflict

Source: https://defensescoop.com/2023/03/21/pentagon-cio-places-high-priority-on-developing-gps-alternatives-with-growing-threat-of-great-power-conflict/

From the Article: "The events that have unfolded over the last year in Ukraine have shown the need to accelerate the fielding of new technologies like GPS alternatives and other forms of satellite communications, John Sherman said."

The Innovation Issue

Source: https://www.technologyreview.com/magazines/the-innovation-issue/

From the Article: "Our annual look at 10 Breakthrough Technologies—including CRISPR for high cholesterol, battery recycling, AI that makes images, and the James Webb Space Telescope—that will have a profound effect on our lives. Plus care robots, 3-D printing pioneers, and chasing bugs on the blockchain."

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 brain waves, this AI can sketch what you're picturing

Source: https://www.nbcnews.com/tech/tech-news/brain-waves-ai-can-sketch-picturing-rcna76096

From the Article: "Researchers around the world are training AI to re-create images seen by humans using only their brain waves. Experts say the technology is still in its infancy, but it heralds a new brain-analysis industry."

CISO MindMap 2023: What do InfoSec Professionals Really do?

Source: https://rafeeqrehman.com/2023/03/25/ciso-mindmap-2023-what-do-infosec-professionals-really-do/

From the Article: "Most people outside the Cybersecurity profession don't fully realize and appreciate the complexity of a security professional's job. Since 2012, CISO MindMap has been an effective educational tool to communicate CISO responsibilities and has enabled security professionals to design and refine their security programs."

What to know about China's new cross-border data transfer security assessment guidelines

Source: https://iapp.org/news/a/what-to-know-about-chinas-new-cross-border-data-transfer-security-assessment-guidelines/

From the Article: "On the eve of the measures coming into force, the Cyberspace Administration of China issued the Guidelines on Application for Security Assessment of Cross-Border Data Transfers (1st Edition) to provide detailed guidance and reference on how to perform the security assessment."

Android app from China executed 0-day exploit on millions of devices

Source: https://arstechnica.com/information-technology/2023/03/android-app-from-china-executed-0-day-exploit-on-millions-of-devices/

From the Article: "Fast-growing e-commerce app Pinduoduo had an EvilParcel stow-away."

Link back to Table of Contents

PCBAA applauds presidential action

Source: https://www.linkedin.com/pulse/pcbaa-applauds-presidential-action/

From the Article: "The recent partnership announced by the U.S. and Canada is a welcome acknowledgement of the urgent need to support the American printed circuit board industry. The Presidential determination of printed circuit boards as essential to national defense under section 303 of the Defense Production Act is welcome news, and achieves a 2023 goal of the Printed Circuit Board Association of America (PCBAA)."

[Editorial] Rocking the World With Advanced Package Technology

Source: https://news.samsung.com/global/editorial-rocking-the-world-with-advanced-package-technology

From the Article: "Governments are also paying close attention. The South Korean Ministry of Trade, Industry and Energy hosted a forum on semiconductor packaging technology in February, while DARPA (Defense Advanced Research Projects Agency) of the US Department of Defense announced the allocation of a large-scale budget for advanced package-related fields last April. The Japanese government also announced new incentives to attract research centers, as well as establishing a dedicated symposium."

Chip Sales Rise in 2022, Especially to Auto, Industrial, Consumer Markets

Source: https://www.semiconductors.org/chip-sales-rise-in-2022-especially-to-auto-industrial-consumer-markets/

From the Article: "Historically, the PC/computer and communication end markets have accounted for approximately two-thirds of overall sales, with sectors such as automotive, industrial, and consumer electronics accounting for the remainder. But sales by end-market in 2022 showed a marked shift, according the 2022 Semiconductor End-Use Survey from the World Semiconductor Trade Statistics (WSTS) organization."

Automotive IoT Security By Design

Source: https://semiengineering.com/automotive-iot-security-by-design/

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: "Monitoring transactions occurring during the boot sequence to protect connected vehicles."

Healthcare Leaders Call for Cybersecurity Standards

Source: https://www.bankinfosecurity.com/senate-hearing-a-21458

From the Article: "Also: Please Help the Sector Pay for Cybersecurity, Execs Tell Senate Panel"

Congress lays groundwork for AUKUS export control reform

Source: https://www.defensenews.com/congress/2023/03/22/congress-lays-groundwork-for-aukus-export-control-reform/

From the Article: "WASHINGTON — Congress on Wednesday took the first step in what is expected to be a lengthy effort to overhaul U.S. export control laws in order to expedite technology cooperation needed to implement a central pillar of the AUKUS trilateral agreement with Australia and the U.K."

'Very concerning': SVB's collapse rattled Pentagon tech hub, prods closer collaboration

Source: https://breakingdefense.com/2023/03/very-concerning-svbs-collapse-rattled-pentagon-tech-hub-prods-closer-collaboration/

From the Article: "The collapse of Silicon Valley Bank is a potential opportunity to grow the "connective tissue" between the Pentagon and the commercial sector and "build a partnership," DIU's Acting Director Mike Madsen said."

AI computing startup Cerebras releases open source ChatGPT-like models

Source: https://www.reuters.com/article/ai-cerebras-languagemodel-idCAKBN2VU12I

From the Article: "OAKLAND, California (Reuters) - Artificial intelligence chip startup Cerebras Systems on Tuesday said it released open source ChatGPT-like models for the research and business community to use for free in an effort to foster more

Link back to Table of Contents

collaboration."

Chips program office releases additional funding application guidance

Source: https://www.semi.org/en/blogs/semi-news/chips-program-office-releases-additional-funding-application-guidance

From the Article: "Pre-Application – The pre-application is optional but strongly recommended because it will enable the CPO to start a dialogue with applicants and provide feedback prior to the submission of full applications. Leading-edge project applicants may submit pre-applications starting March 31, while current-generation, mature-node, and back-end applicants may do so starting May 1. Pre-application materials include the following:"

Innovation Authority collaborates with NY Creates on research

Source: https://www.jpost.com/business-and-innovation/article-735683

From the Article: "A joint declaration signed this week will lead to the integration of Israeli tech and research in NY Create's research activities"

Microsoft Introduces GPT-4 AI-Powered Security Copilot Tool to Empower Defenders

Source: https://thehackernews.com/2023/03/microsoft-introduces-gpt-4-ai-powered.html

From the Article: "Microsoft on Tuesday unveiled Security Copilot in preview, marking its continued push to embed AI-oriented features in an attempt to offer "end-to-end defense at machine speed and scale.""

NSA Releases Recommendations for Maturing Identity, Credential, and Access Management in Z

Source: https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3328152/nsa-releases-recommendations-for-maturing-identity-credential-and-access-manage/

From the Article: "FORT MEADE, Md. - The National Security Agency (NSA) released

the “Advancing Zero Trust Maturity throughout the User Pillar” Cybersecurity Information Sheet (CSI) today to help system operators’ mature identity, credential, and access management (ICAM) capabilities to effectively mitigate certain cyber threat techniques"

IBM expand chip business canada

Source: https://www.gizmochina.com/2023/03/27/ibm-expand-chip-business-canada/

From the Article: "IBM plans to expand its chip business in Canada which will help in creating a bilateral semiconductor corridor between US and Canada. "

Google again accused of destroying evidence in Android case

Source: https://www.theregister.com/2023/03/28/google_destroying_evidence_claim/

From the Article: "Starting to see a pattern here? Judge seems to think so"

Prince Harry says Royal Family 'without doubt' withheld information from him on phone hacking

Source: https://news.sky.com/story/prince-harry-says-royal-family-without-doubt-withheld-information-from-him-on-phone-hacking-12844296

From the Article: "The Duke of Sussex appeared in court for the second day today as he pursues his case against the Daily Mail publisher Associated Newspapers."

Dridex malware, the banking trojan

Source: https://cybersecurity.att.com/blogs/security-essentials/dridex-malware-the-banking-trojan

From the Article: "Dridex, also known as Cridex or Bugat, is a banking Trojan that has been active since 2011. The malware is primarily used to steal sensitive information, such as login credentials and financial information, from victims. Dridex is known for its ability to evade detection by using dynamic configuration files and hiding its servers behind proxy layers."

Link back to Table of Contents

Anomali Cyber Watch: Account takeover, APT, Banking trojans, China, Cyberespionage, India, Malspam, North Korea, Phishing, Skimmers, Ukraine, and Vulnerabilities

Source: https://www.anomali.com/blog/anomali-cyber-watch-account-takeover-apt-banking-trojans-china-cyberespionage-india-malspam-north-korea-phishing-skimmers-ukraine-and-vulnerabilities

From the Article: "The various threat intelligence stories in this iteration of the Anomali Cyber Watch discuss the following topics: Account takeover, APT, Banking trojans, China, Cyberespionage, India, Malspam, North Korea, Phishing, Skimmers, Ukraine, and Vulnerabilities."

Office of the Director of National Intelligence highlights cyber threats in 2023 Intelligence Threat Assessment

Source: https://www.csoonline.com/article/3691619/office-of-the-director-of-national-intelligence-highlights-cyber-threats-in-2023-intelligence-threa.html

From the Article: "When the Office of the Director of National Intelligence (ODNI) highlights a threat in its unclassified assessment and intimates that there is substantive supporting evidence available, one should not sit back and let the data points pass idly by — and we aren't. "

Legacy, password-based authentication systems are failing enterprise security, says study

Source: https://www.csoonline.com/article/3691781/legacy-password-based-authentication-systems-are-failing-enterprise-security-says-study.html

From the Article: "Authentication-related attacks grew in 2022, taking advantage of outdated, password-based authentication systems, according to a study commissioned by HYPR, a passwordless multifactor authentication (MFA) provider based in the US."

Hackers changed tactics, went cross-platform in 2022, says Trend Micro

Source: https://www.csoonline.com/article/3691790/hackers-changed-tactics-went-

Link back to Table of Contents

cross-platform-in-2022-says-trend-micro.html

From the Article: "Payouts from ransomware victims declined by 38% in 2022, prompting hackers to adopt more professional and corporate tactics to ensure higher returns, according to Trend Micro's Annual Cybersecurity Report. "

PwC UK partners with ReversingLabs to bring software supply chain security to third-party risk management

Source: https://www.csoonline.com/article/3691898/pwc-uk-partners-with-reversinglabs-to-bring-software-supply-chain-security-to-third-party-risk-mana.html

From the Article: "Advisory and professional services giant PwC UK is partnering with security firm ReversingLabs to develop a third-party risk management (TPRM) platform to help businesses address software supply chain security risks."

Europol warns of criminal use of ChatGPT

Source: https://securityaffairs.com/144132/cyber-crime/europol-warns-cybercrime-chatgpt.html

From the Article: "EU police body Europol warned about the potential abuse of systems based on artificial intelligence, such as the popular chatbot ChatGPT, for cybercriminal activities."

Nexus, an emerging Android banking Trojan targets 450 financial apps

Source: https://securityaffairs.com/143910/malware/nexus-android-banking-trojan.html

From the Article: "Cybersecurity firm experts from Cleafy warn of an emerging Android banking trojan, named Nexus, that was employed by multiple groups in attacks against 450 financial applications."

North Korean hackers turn to 'cloud mining' for crypto to avoid law enforcement scrutiny

Source: https://cyberscoop.com/north-korean-hackers-cloud-mining-cyrptocurrency/

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 North Korean espionage unit suspected of impersonating journalists and faking LinkedIn accounts to collect intelligence is using a novel way to fund their international hacking operations: renting out cloud-based power to mine for cryptocurrency."

ChatGPT-4 and cyber crime, insights from a Nasdaq TradeTalk

Source: https://www.cybertalk.org/2023/03/28/chatgpt-4-cyber-crime-insights-from-a-nasdaq-tradetalk/

From the Article: "It's a good question. I think that what we've discovered since November of last year, when ChatGPT was first released, is that ChatGPT has really opened the doors to a lot of different things, some of which are positive…and some that we can discuss today."

CLOPS Claim to Have Hacked 130 Organizations

Source: https://www.cysecurity.news/2023/03/clops-claim-to-have-hacked-130.html

From the Article: "It is now reported that the Clop ransomware group - known for its Linux variant recently - has used the zero-day vulnerability of the GoAnywhere MFT file transfer tool that they claim to have hacked into hundreds of organizations to boost its reputation by claiming to have stolen data from hundreds of organizations."

Microsoft Conduct an Emergency Fix for the Notorious 'Acropalypse' Bug

Source: https://www.cysecurity.news/2023/03/microsoft-conduct-emergency-fix-for.html

From the Article: "Recently, Microsoft has acted quickly in patching up the 'acropalypse' bug that was discovered earlier this week. The bug could apparently enable information cropped out of images via the Windows screenshot tools to be recovered. "

Chinese-Designed Apps Pose Greater Privacy Risks to Americans

Source: https://www.cysecurity.news/2023/03/chinese-designed-apps-pose-greater.html

From the Article: "As the US Congress considers a ban on the Chinese social media

app TikTok over security concerns, millions of Americans continue to download Chinese-designed apps that pose even greater privacy risks. Despite this, there has been no outcry from lawmakers or regulators about these apps."

NullMixer Polymorphic Malware Variant Infects 8K Targets in Just a Month

Source: https://www.darkreading.com/attacks-breaches/nullmixer-polymorphic-malware-variant-8k-targets-month

From the Article: "The NullMixer loader has compromised thousands of endpoints in the US, France, and Italy, stealing data and selling it to Dark Web data dealers, all without setting off alarm bells."

Hacker Returns $200 Million Stolen from Euler Finance

Source: https://www.hackread.com/hacker-returns-200-million-euler-finance/

From the Article: "Euler Finance was hacked on March 13, 2023, and around $197 million worth of cryptocurrency was stolen, including $135.8 million stETH, $33.8 million USDC, $18.5 million WBTC, and $8.7 million DAI."

Prompt engineering and jailbreaking: Europol warns of ChatGPT exploitation

Source: https://www.hackread.com/europol-chatgpt-prompt-engineering-jailbreaking/

From the Article: "The concern arises from the growing number of cybercriminals attempting to exploit the AI-based chatbot for developing malware and other malicious tools."

Pwn2Own 2023: Tesla Model 3, Windows 11, Ubuntu and more Pwned

Source: https://www.hackread.com/pwn2own-2023-tesla-windows-11-ubuntu-pwned/

From the Article: "This year's Pwn2Own 2023 was held in Vancouver between March 22nd and 24th, 2023."

Link back to Table of Contents

Phishing Campaign Goes Cutting Edge With IPFS

Source: https://www.bankinfosecurity.com/phishing-campaign-goes-cutting-edge-ipfs-a-21553

From the Article: "Attackers Using Decentralized File Protocol to Deliver Phishing Pages Credential harvesting attackers are taking advantage of a distributed file protocol to distribute customized phishing links. "

North Korean Threat Groups Steal Crypto to Pay for Hacking

Source: https://www.bankinfosecurity.com/north-korean-threat-groups-steal-crypto-to-pay-for-hacking-a-21548

From the Article: "North Korean hackers are stealing cryptocurrency to fund operations under an apparent mandate from Pyongyang to be self sufficient, threat intel firm Mandiant says. The regime probably expected its hackers to pay their own way before 2020, but the novel coronavirus pandemic exacerbated its demands."

Partnering for Better Cloud Security: Enhanced Threat Detection and Response

Source: https://www.bankinfosecurity.com/webinars/partnering-for-better-cloud-security-enhanced-threat-detection-response-w-4768

From the Article: "Join us for a webinar on how cloud security will bring together leading technologies to provide comprehensive cloud security solutions. Through collaboration, we will discuss how to enhance cloud security measures by combining technologies to provide enhanced discovery, visibility, prioritization, and response capabilities, real-time cloud threat detection, and risk assessments. "

NY AG Hits Law Firm With $200K Settlement in Health Breach

Source: https://www.bankinfosecurity.com/ny-ag-hits-law-firm-200k-settlement-in-health-breach-a-21539

From the Article: "A New York medical malpractice law firm will pay $200,000 and implement data security improvements to settle a HIPAA enforcement action by the state attorney general's office following a 2021 ransomware attack by LockBit."

Link back to Table of Contents

Ransomware Groups Seek Fresh Tactics Following Hive Takedown

Source: https://www.bankinfosecurity.com/stung-by-hive-takedown-ransomware-groups-seek-fresh-tactics-a-21533

From the Article: "Stung by the FBI's infiltration and takedown of the Hive ransomware group, other ransomware operators have been retooling their approaches to make their attacks more effective and operations tougher to disrupt, says Yelisey Bohuslavskiy, chief research officer at threat intelligence firm Red Sense."

Exchange Online will soon start blocking emails from old, vulnerable on-prem servers

Source: https://www.helpnetsecurity.com/2023/03/28/exchange-online-blocking-emails-from-vulnerable-servers/

From the Article: "Slowly but surely, Microsoft aims to make it impossible for unsupported and/or unpatched on-prem Microsoft Exchange servers to use the company's Exchange Online hosted cloud service to deliver email."

Endace collaborates with Niagara Networks to accelerate response to network threats

Source: https://www.helpnetsecurity.com/2023/03/29/endace-niagara-networks/

From the Article: "Endace and Niagara Networks announced a partnership that combines Endace's scalable, always-on packet capture with Niagara Networks' complete visibility solutions. "

Tausight expands its AI-based PHI Security Intelligence platform to cover new attack vectors

Source: https://www.helpnetsecurity.com/2023/03/28/tausight-phi-security-intelligence/

From the Article: "Tausight has expanded its AI-based PHI Security Intelligence platform which automates the discovery and identification of electronic PHI to enhance the protection of healthcare patients' most valuable confidential information."

Link back to Table of Contents

Motivations for Insider Threats: What to Watch Out For

Source: https://www.tripwire.com/state-of-security/motivations-insider-threats-what-watch-out

From the Article: "While a majority of discourse in the cybersecurity industry is focused on external threats – malicious hacking, phishing, and the like – the fact is that internal actors are just as capable of causing damage to an enterprise, if not more so."

Two-Week ATO Attack Mitigated by Imperva

Source: https://www.imperva.com/blog/two-week-ato-attack-mitigated-by-imperva/

From the Article: "Beginning on February 7, an Imperva-protected account was targeted by an ongoing account takeover (ATO) attack that lasted for two weeks. On average, attacks last a few hours or a couple days at most, so the length of this attack was an anomaly and underscores the persistence of the attackers. "

ENISA releases ECSMAF v2.0 to analyze EU cybersecurity market, improve guidance to cybersecurity stakeholders

Source: https://industrialcyber.co/regulation-standards-and-compliance/enisa-releases-ecsmaf-v2-0-to-analyze-eu-cybersecurity-market-improve-guidance-to-cybersecurity-stakeholders/

From the Article: "The European Union Agency for Cybersecurity (ENISA) released Monday a ‘cornerstone’ document of the agency’s activities in analyzing the European Union cybersecurity market, presenting an updated cybersecurity market analysis framework, with guidance on how EU cybersecurity market analyses can be performed."

WEF initiates multi-stakeholder community to strengthen cyber resilience across manufacturing ecosystem

Source: https://industrialcyber.co/manufacturing/wef-initiates-multi-stakeholder-community-to-strengthen-cyber-resilience-across-manufacturing-ecosystem/

From the Article: "The World Economic Forum (WEF) is convening a multistakeholder community to strengthen cyber resilience across the whole manufacturing ecosystem, as the sector remains the ‘most targeted sector’ by 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.

Cymulate's 2022 Cybersecurity Effectiveness Report reveals that organizations are leaving common attack paths exposed

Source: https://www.itsecurityguru.org/2023/03/28/cymulates-2022-cybersecurity-effectiveness-report-reveals-that-organizations-are-leaving-common-attack-paths-exposed-in-their-quest-to-combat-emergent-threats/

From the Article: "Cymulate, the leader in cybersecurity risk validation and exposure management, today released the company's "2022 Cybersecurity Effectiveness Report" which analyzed the results of over a million security posture validation assessments, including 1.7 million hours of offensive cybersecurity testing within Cymulate's production environments."

CyberheistNews Vol 13 #13 [Eye Opener] How to Outsmart Sneaky AI-Based Phishing Attacks

Source: https://blog.knowbe4.com/cyberheistnews-vol-13-13-eye-opener-how-to-outsmart-sneaky-ai-based-phishing-attacks

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."

Oversharing Is a Risk to Information Security

Source: https://blog.knowbe4.com/oversharing-risk-to-information-security

From the Article: "Younger employees need to be wary of oversharing company information on social media, according to John Karabin, senior director of cybersecurity at NTT Ltd. In an article for SmartCompany, Karabin explained that while younger users are typically more acclimated to new technologies, they may also be more distracted by them."

Bay Area Bank Collapse and the Cybersecurity Impact

Source: https://www.trendmicro.com/en_us/ciso/23/c/bay-area-bank-collapse-

Link back to Table of Contents

cybersecurity-impact.html

From the Article: "Greg Young, VP of Cybersecurity and CorpDev, discusses what the second-largest bank collapse in U.S. history means for cybersecurity."

Earth Preta's Cyberespionage Campaign Hits Over 200

Source: https://www.trendmicro.com/en_us/research/23/c/earth-preta-cyberespionage-campaign-hits-over-200.html

From the Article: "We present a case study of the cyberespionage efforts by Earth Preta. This study on an active campaign delves into the structure, goals, and requirements of the organizations involved, and provides an opportunity to conduct wider intelligence analysis and insights in the development of effective countermeasures."

Gone in 120 seconds: Tesla Model 3 child's play for hackers

Source: https://www.theregister.com/2023/03/27/in_brief_security/

From the Article: "In brief A team of hackers from French security shop Synacktiv have won $100,000 and a Tesla Model 3 after subverting the Muskmobile's entertainment system, and from there opening up the car's core management systems."

Stealthy DBatLoader Malware Loader Spreading Remcos RAT and Formbook in Europe

Source: https://thehackernews.com/2023/03/stealthy-dbatloader-malware-loader.html

From the Article: "A new phishing campaign has set its sights on European entities to distribute Remcos RAT and Formbook via a malware loader dubbed DBatLoader."

Pakistan-Origin SideCopy Linked to New Cyberattack on India's Ministry of Defence

Source: https://thehackernews.com/2023/03/pakistan-origin-sidecopy-linked-to-new.html

From the Article: "An advanced persistent threat (APT) group that has a track record of

targeting India and Afghanistan has been linked to a new phishing campaign that delivers Action RAT."

20-Year-Old BreachForums Founder Faces Up to 5 Years in Prison

Source: https://thehackernews.com/2023/03/20-year-old-breachforums-founder-faces.html

From the Article: "Conor Brian Fitzpatrick, the 20-year-old founder and the administrator of the now-defunct BreachForums has been formally charged in the U.S. with conspiracy to commit access device fraud."

Chinese cyberespionage in the Middle East. North Korea's APT43. Phishing in China's nuclear energy sector.

Source: https://thecyberwire.com/newsletters/research-briefing/5/13

From the Article: "Chinese cyberespionage in the Middle East. North Korea's APT43. Phishing in China's nuclear energy sector."

DPRK hacks for cash and intelligence. Twitter's source-code leak. Data security and resilience. Hacktivist auxiliary updates.

Source: https://thecyberwire.com/newsletters/daily-briefing/12/59

From the Article: "Cyberespionage and cybercrime in the interest of Pyongyang’s weapons programs. Twitter gets a subpoena for source-code leaker’s information. Survey on the state of resilience. "

ChatGPT Data Breach Confirmed as Security Firm Warns of Vulnerable Component Exploitation

Source: https://www.securityweek.com/chatgpt-data-breach-confirmed-as-security-firm-warns-of-vulnerable-component-exploitation/

From the Article: "OpenAI has confirmed a ChatGPT data breach on the same day a security firm reported seeing the use of a component affected by an actively exploited

vulnerability."

China's Nuclear Energy Sector Targeted in Cyberespionage Campaign

Source: https://www.securityweek.com/chinas-nuclear-energy-sector-targeted-in-cyberespionage-campaign/

From the Article: "A South Asian espionage group named Bitter has been observed targeting the Chinese nuclear energy sector."

Microsoft: No-Interaction Outlook Zero Day Exploited Since Last April

Source: https://www.securityweek.com/microsoft-no-interaction-outlook-zero-day-exploited-since-last-april/

From the Article: "Microsoft says it has evidence that Russian APT actors were exploiting a nasty Outlook zero-day as far back as April 2022, upping the stakes on organizations to start hunting for signs of compromise."

New SIA Map Highlights Broad U.S. Semiconductor Ecosystem

Source: https://www.semiconductors.org/new-sia-map-highlights-broad-u-s-semiconductor-ecosystem/

From the Article: "The semiconductor ecosystem in the United States is broad and diverse, as illustrated by SIA's new U.S. Semiconductor Ecosystem Map, a first-of-its-kind tool that allows users to explore industry activities across the country, including nearly 500 locations in 42 states."

Attackers Could Exploit Flaw in WiFi Protocol to Hijack TCP Connections

Source: https://www.blackhatethicalhacking.com/news/attackers-could-exploit-flaw-in-wifi-protocol-to-hijack-tcp-connections/

From the Article: "Cybersecurity researchers have found a significant vulnerability in the IEEE 802.11 WiFi protocol standard, which can be exploited by hackers to trick access points into leaking network frames in plaintext form."

Link back to Table of Contents

3CX Supply Chain Compromise Leads to ICONIC Incident

Source: https://www.volexity.com/blog/2023/03/30/3cx-supply-chain-compromise-leads-to-iconic-incident/

From the Article: "On Wednesday, March 29, 2023, Volexity became aware of a supply chain compromise by a suspected North Korean threat actor, which Volexity tracks as UTA0040*."

Top Vulnerabilities in 2023 and How to Block Them

Source: https://blog.checkpoint.com/2023/03/30/top-vulnerabilities-in-2023-and-how-to-block-them/

From the Article: "Before cyber attackers can wage successful malware or ransomware campaigns, they have to gain access to their target environments. "

3CXDesktop App Trojanizes in A Supply Chain Attack: Check Point Customers Remain Protected

Source: https://blog.checkpoint.com/2023/03/29/3cxdesktop-app-trojanizes-in-a-supply-chain-attack-check-point-customers-remain-protected/

From the Article: "The application allows users to communicate within and outside the organization through their desktop or laptops."

DXC Technology says global network is not compromised following Latitude Financial breach

Source: https://www.csoonline.com/article/3692292/dxc-technology-says-global-network-is-not-compromised-following-latitude-financial-breach.html

From the Article: "Soon after Latitude Financial revealed it suffered a cyber attack, DXC Technology quietly published a note on its website stating its global network and customer support networks were not compromised."

Link back to Table of Contents

Latin American companies, governments need more focus on cybersecurity

Source: https://www.csoonline.com/article/3691780/latin-american-companies-governments-need-more-focus-on-cybersecurity.html

From the Article: "More than 200 CISOs in the Americas region, in addition to the Inter-American Development Bank (IDB), Latin American Federation of Banks (FELABAN), and the World Economic Forum (WEF), contributed to the report."

Spera exits stealth to reveal identity-based threat hunting capabilities

Source: https://www.csoonline.com/article/3691795/spera-exits-stealth-to-reveal-identity-based-threat-hunting-capabilities.html

From the Article: "The Israeli identity-based cybersecurity provider Spera is exiting stealth mode to reveal a namesake offering with identity security posture management (ISPM) capabilities."

Skyhawk adds ChatGPT functions to enhance cloud threat detection, incident discovery

Source: https://www.csoonline.com/article/3691654/skyhawk-adds-chatgpt-functions-to-enhance-cloud-threat-detection-incident-discovery.html

From the Article: "Cloud threat detection and response (CDR) vendor Skyhawk has announced the incorporation of ChatGPT functionality in its offering to enhance cloud threat detection and security incident discovery. "

Mélofée: New Linux Malware Found by Researchers With Links to Chinese APT Groups

Source: https://cyberintelmag.com/malware-viruses/melofee-new-linux-malware-found-by-researchers-with-links-to-chinese-apt-groups/

From the Article: "A new piece of malware targeted targeting Linux systems has been connected to an unidentified Chinese state-sponsored hacking gang. ExaTrack, a French cybersecurity company, discovered three instances of the previously reported dangerous software in early 2022 and gave it the name Mélofée."

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

Google reveals two global spyware campaigns targeting Apple and Android devices

Source: https://cyberscoop.com/google-tag-spyware-android-ios-chrome/

From the Article: "Google's Threat Analysis Group on Wednesday revealed two "limited and highly targeted" spyware campaigns that took advantage of zero-day vulnerabilities as well as known but unpatched security holes to undermine protections on Android and Apple iOS devices as well as Google's Chrome browser."

How Threat Actors are Using IPFS for Email Phishing

Source: https://www.cysecurity.news/2023/03/how-threat-actors-are-using-ipfs-for.html

From the Article: "InterPlanetary File System (IPFS) is a peer-to-peer distributed file system, that allows users around the world to exchange files. Instead of using file paths for addressing like centralized systems do, IPFS uses unique content identifiers (CID). The file itself stays on the user's computer which had "uploaded" it to IPFS and downloaded directly from the computer. "

Pinduoduo Malware Executed a Dangerous 0-day Exploit Against Millions of Android Devices

Source: https://www.cysecurity.news/2023/03/pinduoduo-malware-executed-dangerous-0.html

From the Article: "In accordance with a new report, Pinduoduo, a popular Chinese shopping app, exploited a zero-day vulnerability in the Android operating system to uplift its own privileges, rob personal data from infected endpoints, and install malicious apps. "

Improper Disposal of IT Equipment Poses Cyber Security Risks

Source: https://www.cysecurity.news/2023/03/improper-disposal-of-it-equipment-poses.html

From the Article: "As technology continues to advance at a rapid pace, it is no surprise that electronic waste, or e-waste, has become a growing concern. With many

companies constantly upgrading their IT equipment, the amount of electronic waste being produced is on the rise. "

How to Keep Up With a Shifting Threat Landscape

Source: https://www.cysecurity.news/2023/03/how-to-keep-up-with-shifting-threat.html

From the Article: "Cybercrime is a problem that is only escalating and is bad for business, as one might anticipate. Regardless of how you feel about it, it forces your business to take action in order to secure its infrastructure."

Using Observability to Power a Smarter Cybersecurity Strategy

Source: https://www.darkreading.com/vulnerabilities-threats/using-observability-to-power-a-smarter-cybersecurity-strategy

From the Article: "With an infrastructure for observability, security teams can make better decisions about access and identity-based threats."

Top Tech Talent Warns of AI's Threat to Human Existence in Open Letter

Source: https://www.darkreading.com/application-security/top-tech-talent-ai-threat-human-existence-open-letter

From the Article: "Elon Musk, Steve Wozniak, and Andrew Yang are among more than 1,000 tech leaders asking for time to establish human safety parameters around AI."

Cybersecurity Investment Outlook Remains Grim as Funding Activity Sharply Declines

Source: https://www.darkreading.com/threat-intelligence/cybersecurity-investment-and-m-a-activity-slowed-in-q1-2023

From the Article: "Security analysts expect little improvement until at least the second half of the year."

Link back to Table of Contents

Google: Commercial Spyware Used by Governments Laden With Zero-Day Exploits

Source: https://www.darkreading.com/attacks-breaches/google-spyware-governments-zero-day-exploits

From the Article: "Google TAG researchers reveal two campaigns against iOS, Android, and Chrome users that demonstrate how the commercial surveillance market is thriving despite government-imposed limits."

Phishing Emails Up a Whopping 569% in 2022

Source: https://www.darkreading.com/attacks-breaches/phishing-emails-up-whopping-569-percent-2022

From the Article: "Credential phishing emails are the clear favorite of threat actors, with a 478% spike last year, new research shows."

US threatens to ban TikTok unless Chinese owners divest

Source: https://www.theguardian.com/technology/2023/mar/15/us-joe-biden-tiktok-ban-chinese-owners-divest

From the Article: "The Biden administration has threatened to ban TikTok in the US unless the social media company's Chinese owners divest their stakes in it, according to news reports on Wednesday."

Ransomware Roundup – Dark Power and PayMe100USD Ransomware

Source: https://www.fortinet.com/blog/threat-research/dark-power-and-payme100usd-ransomware

From the Article: "In this week's Ransomware Roundup, FortiGuard Labs covers the Dark Power and PayME100USD ransomware along with protection recommendations. "

Meeting Cybersecurity Insurance Requirements and Protecting Privileged Access

Source: https://www.fortinet.com/blog/business-and-technology/cybersecurity-

Link back to Table of Contents

insurance-and-protecting-priviledged-access

From the Article: "With Fortinet's release of FortiPAM, organizations can now more easily meet requirements for cybersecurity insurance."

Moobot Strikes Again - Targeting Cacti And RealTek Vulnerabilities

Source: https://www.fortinet.com/blog/threat-research/moobot-strikes-again-targeting-cacti-and-realtek-vulnerabilities

From the Article: "FortiGuard Labs examined several attacks targeting Cacti and Realtek vulnerabilities. Understand the payloads of these attacks and their resulting behavior of spreading ShellBot and Moobot malware."

Spyware Vendors Exploit 0-Days On Android and iOS Devices

Source: https://gbhackers.com/spyware-vendors-exploit-0-days/

From the Article: "The Threat Analysis Group (TAG) of Google unveiled recently that commercial spyware vendors targeted Android and iOS devices using zero-day vulnerabilities patched last year."

New WiFi Flaw Let Attackers Hijack Network Traffic

Source: https://gbhackers.com/new-wifi-flaw/

From the Article: "A fundamental security issue in the design of the IEEE 802.11 WiFi protocol standard, according to a technical study written by Domien Schepers, Aanjhan Ranganathan, and Mathy Vanhoef of imec-DistriNet, KU Leuven, allows attackers to deceive access points into exposing network frames in plaintext."

Google reveals spyware attack on Android, iOS, and Chrome

Source: https://www.hackread.com/google-spyware-attack-android-ios-chrome/

From the Article: "Google's Threat Analysis Group (TAG) labeled the spyware campaign as limited but highly 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.

Mélofée: The Latest Malware Targeting Linux Servers

Source: https://www.hackread.com/melofee-latest-malware-targeting-linux/

From the Article: "An unidentified Chinese APT group is suspected of operating the Mélofée malware."

Ransomware Groups Hit Unpatched IBM File Transfer Software

Source: https://www.bankinfosecurity.com/ransomware-groups-hit-unpatched-ibm-file-transfer-software-a-21569

From the Article: "Security experts are urging users of IBM's Aspera Faspex file-exchange application to take it offline immediately unless they've patched a flaw being actively exploited by ransomware groups, including Buhti and IceFire."

Phishing Campaign Tied to Russia-Aligned Cyberespionage

Source: https://www.bankinfosecurity.com/phishing-campaign-tied-to-russia-aligned-cyberespionage-a-21567

From the Article: "A hacking group with apparent ties to Russia or Belarus has been using "simple yet effective attack techniques and tools" to gain access to multiple governments' email systems, as part of apparent cyberespionage operations in support of Russia's invasion of Ukraine, researchers warn."

Cisco Buys Startup Lightspin to Address Cloud Security Risks

Source: https://www.bankinfosecurity.com/cisco-buys-startup-lightspin-to-address-cloud-security-risks-a-21560

From the Article: "Cisco plans to purchase its second cloud security startup in two months to deliver context, prioritization and remediation recommendations for cloud native resources."

Link back to Table of Contents

Command-and-Control Servers Explained. Techniques and DNS Security Risks

Source: https://heimdalsecurity.com/blog/command-and-control-servers-explained/

From the Article: "A command-and-control server (C&C) is a computer that threat actors use to send instructions to compromised systems."

The best defense against cyber threats for lean security teams

Source: https://www.helpnetsecurity.com/2023/03/30/best-defense-against-cyber-threats-lean-security-teams/

From the Article: "H0lyGh0st, Magecart, and a slew of state-sponsored hacker groups are diversifying their tactics and shifting their focus to… you. That is, if you're in charge of cybersecurity for a small-to-midsize enterprise (SME). "

TXOne reports critical infrastructures face large-scale ransomware attacks, as 94% of IT security incidents impact OT

Source: https://industrialcyber.co/reports/txone-reports-critical-infrastructures-face-large-scale-ransomware-attacks-as-94-of-it-security-incidents-impact-ot/

From the Article: "Data published Wednesday by Trend Micro's OT security arm TXOne Networks identified a heightened frequency of cyberattacks on key industry suppliers, especially those in the energy and critical manufacturing sectors in 2022."

Cyberspace Solarium Commission makes four recommendations to Congress to enhance maritime cybersecurity

Source: https://industrialcyber.co/transport/cyberspace-solarium-commission-makes-four-recommendations-to-congress-to-enhance-maritime-cybersecurity/

From the Article: "Cyberspace Solarium Commission published Tuesday a report providing additional analysis of cyberattacks against the maritime transportation system (MTS) with recommendations to the U.S. Congress to resource the subsector's cybersecurity more fully. It also highlights the need for better government-industry cybersecurity collaboration and better resourcing of government efforts to support the private sector. "

Link back to Table of Contents

NanoLock Security, ISTARI push device level OT cyber protection, meet emerging global federal guidelines

Source: https://industrialcyber.co/vendor/nanolock-security-istari-push-device-level-ot-cyber-protection-meet-emerging-global-federal-guidelines/

From the Article: "Device-level zero-trust OT cybersecurity company NanoLock Security aligned with ISTARI to provide ISTARI's clients with NanoLock's device-level zero trust OT (operational technology) protection against cyber threats caused by internal and external adversaries."

US Gives Costa Rica $25M For Eradication Of Conti Ransomware

Source: https://informationsecuritybuzz.com/us-gives-costa-rica-25m-eradication-conti-ransomware/

From the Article: "The US provides $25 million to Costa Rica for the eradication of Conti ransomware. To aid the nation in recovering from a devastating ransomware attack that rendered numerous crucial agencies inoperable last year, the US government is handing the government of Costa Rica $25 million."

Barracuda Ransomware Report

Source: https://informationsecuritybuzz.com/barracuda-ransomware-report/

From the Article: "Barracuda Networks, Inc., a trusted partner and leading provider of cloud-first security solutions, today published its 2023 Ransomware Insights report, which shows that 73% of the organisations surveyed report being hit with at least one successful ransomware attack in 2022 — and 38% say they were hit twice or more."

North Korean Hackers Use Trojanized 3CX DesktopApp in Supply Chain Attacks

Source: https://www.infosecurity-magazine.com/news/north-korea-hackers-trojanized-3cx/

From the Article: "Windows and Mac versions of the software were compromised to deliver infostealers."

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.

Volume of HTTPS Phishing Sites Surges 56% Annually

Source: https://www.infosecurity-magazine.com/news/volume-https-phishing-sites-surges/

From the Article: "Scammers are increasingly trying to legitimize their efforts."

Google Warns Against Commercial Spyware Exploiting Zero-Days

Source: https://www.infosecurity-magazine.com/news/google-warns-spyware-zero-days/

From the Article: "Spyware vendors facilitated the spread of malware by government-backed threat actors."

Clop Ransomware Group Exploits GoAnywhere MFT Flaw

Source: https://www.infosecurity-magazine.com/news/clop-ransomware-exploits/

From the Article: "The vulnerability has a CVSS score of 7.2 and was exploited against several companies in the US."

Attacks Targeting APIs Increased By 400% in Last Six Months

Source: https://www.infosecurity-magazine.com/news/api-attacks-increase-400-last-six/

From the Article: "The new Salt Security report found that 80% of attacks happened over authenticated APIs."

Microsoft Creates GPT-4 AI Assistant for Cybersecurity

Source: https://www.itgovernanceusa.com/blog/microsoft-creates-gpt-4-ai-assistant-for-cybersecurity

From the Article: "You just can't get away from artificial intelligence at the moment.

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, which recently announced the release of a machine learning assistant for Office apps, has added to its repertoire this week with Security Copilot."

New API Report Shows 400% Increase in Attackers

Source: https://www.itsecurityguru.org/2023/03/29/new-api-report-shows-400-increase-in-attackers/

From the Article: "Today Salt Security have released the findings from their latest Salt Labs State of API Security Report, Q1 2023, which found that there has been a 400% increase in unique attackers (over 4800) in the last six months."

ELECOM WAB-MAT registers its windows service executable with an unquoted file path

Source: https://jvn.jp/en/jp/JVN35246979/

From the Article: "WAB-MAT provided by ELECOM CO.,LTD. registers its windows service executable with an unquoted file path."

Artificial Intelligence Makes Phishing Text More Plausible

Source: https://blog.knowbe4.com/ai-makes-phishing-text-more-plausible

From the Article: "Cybersecurity experts continue to warn that advanced chatbots like ChatGPT are making it easier for cybercriminals to craft phishing emails with pristine spelling and grammar, the Guardian reports."

Can AWS Be Hacked? What You Need to Know

Source: https://latesthackingnews.com/2023/03/30/can-aws-be-hacked-what-you-need-to-know/

From the Article: "Amazon Web Services dominates the cloud computing sector and hosts crucial data for businesses of all sizes. But, unfortunately, cybercriminals frequently use fresh and inventive methods to compromise even the most secure systems."

Link back to Table of Contents

6 Malware Removal Tips for Mac

Source: https://latesthackingnews.com/2023/03/30/6-malware-removal-tips-for-mac/

From the Article: "As secure as Apple devices are, unfortunately, there's no guaranteed way to ensure that they won't fall foul of malware sneaking its way onto the devices from time to time. For those of you with a Mac, you'll likely want to ensure that your device stays clean and free from harmful malware and in this guide, we'll be sharing 6 helpful tips to assist with the removal of malware and viruses from your Apple product."

Hackers Used Spyware Made In Spain To Target Users In The UAE

Source: https://techcrunch.com/2023/03/29/hackers-variston-spyware-uae-google/

From the Article: "In a report published on Wednesday, Google's Threat Analysis Group (TAG) said it discovered hackers targeting people in the UAE who used Samsung's native Android browser, which is a customized version of Chromium. The hackers used a set of vulnerabilities chained together and delivered via one-time web links sent to the targets by text message."

ChatGPT happy to write ransomware, just really bad at it

Source: https://www.malwarebytes.com/blog/news/2023/03/chatgpt-happy-to-write-ransomware-just-really-bad-at-it

From the Article: "I've never done it before, and I can't code in C, the language ransomware is mostly commonly written in, but I have a reasonably good idea of what ransomware does."

White House Looks to Secure Space from Cyber Threats

Source: https://www.nextgov.com/cybersecurity/2023/03/white-house-looks-secure-space-cyber-threats/384570/

From the Article: "The Office of the National Cyber Director, the National Space Council and leaders from the private sector laid out next steps to digitally secure the space ecosystem."

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.

Pro-Russian Hackers Target Elected US Officials Supporting Ukraine

Source: https://arstechnica.com/information-technology/2023/03/pro-russian-hackers-target-elected-us-officials-supporting-ukraine/

From the Article: "Threat actors aligned with Russia and Belarus are targeting elected US officials supporting Ukraine, using attacks that attempt to compromise their email accounts, researchers from security firm Proofpoint said."

Ransomware Crooks Are Exploiting IBM File Exchange Bug

Source: https://arstechnica.com/information-technology/2023/03/ransomware-crooks-are-exploiting-ibm-file-exchange-bug-with-a-9-8-severity/

From the Article: "Threat actors are exploiting a critical vulnerability in an IBM file-exchange application in hacks that install ransomware on servers, security researchers have warned."

North Dakota To Require Cybersecurity Education In Public Schools

Source: https://www.scmagazine.com/news/careers/north-dakota-require-cybersecurity-education-public-schools

From the Article: "North Dakota became the first state in the U.S. to require public schools to teach cybersecurity and computer science. Republican Gov. Doug Burgum signed the new law on March 24."

Seventy-three percent of SMBs pay up after a ransomware attack

Source: https://www.watchguard.com/wgrd-news/blog

From the Article: "SMBs account for 99% of all businesses in the USA, and create 1.5 million new jobs every year, 64% of the total. This means that SMBs are a true economic powerhouse in the States. Although many of these companies believe that they are too small to be attacked by cybercriminals, almost half of all cyberattacks in the world target this kind of business."

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

Three decades of cybersecurity vulnerabilities

Source: https://www.pandasecurity.com/en/mediacenter/panda-security/three-decades-vulnerabilities/

From the Article: "Cybercrime trends are always changing. In the 30 years since Panda Security was founded, we've seen everything from computer viruses delivered from floppy disks, malicious attachments, Trojans and ransomware, to live hacking and fileless threats."

Risk Fact #3: Initial Access Brokers Attack What Organizations Ignore

Source: https://blog.qualys.com/vulnerabilities-threat-research/2023/03/30/risk-fact-3-initial-access-brokers-attack-what-organizations-ignore

From the Article: " The front end of attacks – planning and executing penetration of vulnerable IT – is increasingly done by a different threat actor called an Initial Access Broker (IAB). In the 2023 Qualys TruRisk Research Report, Risk Fact #3 addresses the urgent need for organizations to quicken the pace of patching vulnerabilities leveraged by IABs for successful penetrations."

Patch Now: Cybercriminals Set Sights on Critical IBM File Transfer Bug - Dark Reading

Source: https://www.darkreading.com/vulnerabilities-threats/patch-now-cybercriminals-set-sights-critical-ibm-file-transfer-bug

From the Article: "In February, an unknown threat actor used it to deploy Buhti ransomware, after the Shadowserver Foundation picked up on live attempts."

Hacking Incidents Reported by Atlantic General and Lawrence General Hospitals

Source: https://www.hipaajournal.com/hacking-incidents-reported-by-atlantic-general-and-lawrence-general-hospitals/

From the Article: "Atlantic General Hospital (AGH) in Berlin, MD, has recently reported a ransomware attack to the Maine Attorney General that has affected up to 30,704

Link back to Table of Contents

individuals. The attack was detected on January 29, 2023, when files were discovered to have been encrypted."

Ransomware Attacks Target Critical Infrastructure – And It's Paying Off - SDxCentral

Source: https://www.sdxcentral.com/articles/news/ransomware-attacks-target-critical-infrastructure-and-its-paying-off/2023/03/

From the Article: "As such, ransomware attacks target those with the largest possible impact — notably, critical infrastructure organizations and IT, technology, and telecom companies — as they're more likely to fork over the ransom than suffer the broad-reaching consequences of a takedown or widespread loss of sensitive data."

Ransomware, malware attacks rise in 2022: report - The Economic Times

Source: https://economictimes.indiatimes.com/tech/technology/ransomware-malware-attacks-rise-in-2022-report/articleshow/99094491.cms

From the Article: "Ransomware and malware attacks are up even as Indian enterprises continue to increase investments in cybersecurity."

Crackdown on ransomware gangs yet to show an impact: OpenText - IT World Canada

Source: https://www.itworldcanada.com/article/crackdown-on-ransomware-gangs-yet-to-show-an-impact-opentext/534787

From the Article: "Law enforcement triumphs over the Hive, Conti and REvil ransomware gangs in the last 12 months haven't blunted the use of the technology, says a new report from OpenText."

Most people say they would refuse ransomware demands - Accounting Today

Source: https://www.accountingtoday.com/news/vast-majority-say-they-would-balk-at-ransomware-demands-refuse-to-pay

From the Article: "A staff accountant clicked a bad link and now the firm's entire systems have been locked by a ransomware gang. The hackers tell firm leaders that if they ever

want to see their precious data again, they must pay an exorbitant ransom, likely denominated in cryptocurrency so as to make them that much harder to track."

Washington County commissioners amend sheriff's office budget after ransomware incident

Source: https://www.mypanhandle.com/news/local-news/washington-county/washington-county-commissioners-amend-sheriffs-office-budget-after-ransomware-incident/

From the Article: "Washington County commissioners are trying to revamp security after last month's ransomware attack on the sheriff's office computer system."

38% of organisations hit with ransomware in 2022 were repeat victims - ZAWYA

Source: https://www.zawya.com/en/press-release/research-and-studies/38-of-organisations-hit-with-ransomware-in-2022-were-repeat-victims-bthiok3v

From the Article: "The contents of this press release was provided from an external third party provider. This website is not responsible for, and does not control, such external content. This content is provided on an "as is" and "as available" basis and has not been edited in any way."

Ransomware here to stay, but victims keep quiet about attacks | ITWeb

Source: https://www.itweb.co.za/content/Gb3Bw7WagOnq2k6V

From the Article: "Outlining the findings of Arctic Wolf research among cyber security professionals around the world, Jason Oehley, regional manager at Arctic Wolf South Africa, said: "Ransomware is a trend that's here to stay."

BMW France claimed as Play ransomware victim - Cybernews

Source: https://cybernews.com/news/bmw-france-data-breach-ransomware-victim/

From the Article: "Usually, organizations appear on a ransomware gang's site after threat actors have breached a company and stolen its data."

Link back to Table of Contents

Data stolen from Florida sheriff's office leaked by LockBit ransomware group

Source: https://therecord.media/florida-sheriff-data-leak-lockbit-ransomware

From the Article: "The LockBit ransomware group has leaked data it stole from Washington County Sheriff's Office in northeastern Florida."

Prasenjit Saha, LTIMindtree on the need of cyber resilient ransomware protection - ET CIO

Source: https://cio.economictimes.indiatimes.com/news/strategy-and-management/prasenjit-saha-ltimindtree-on-the-need-of-cyber-resilient-ransomware-protection/99076454

From the Article: "Businesses today understand that cyberattacks are inevitable and it's crucial to have a business continuity plan in place. With the advent of digital transformation, organizations have been moving their data and applications to hybrid and multi-cloud environments."

45% of Indian organizations hit with ransomware in 2022 were repeat victims - APN News

Source: https://www.apnnews.com/45-of-indian-organizations-hit-with-ransomware-in-2022-were-repeat-victims/

From the Article: "Barracuda Networks, Inc., a trusted partner and leading provider of cloud-first security solutions, today published its 2023 Ransomware Insights report, which shows that 73% of the Indian organizations surveyed report being hit with at least one successful ransomware attack in 2022 — and 45% say they were hit twice or more."

Inside ransomware's organised underworld - BCS, The Chartered Institute for IT

Source: https://www.bcs.org/articles-opinion-and-research/inside-ransomware-s-organised-underworld/

From the Article: "Beyond their recent foray into the hipster end of the milk and cheese

Link back to Table of Contents

market, it transpires that goats can teach us a thing or two about cyber security and how successful cyber attacks are carried out."

Lockbit ransomware gang infrastructure reported down | Cybernews

Source: https://cybernews.com/news/lockbit-ransomware-gang-infrastructure-reported-down/

From the Article: "A known ransomware monitoring website is reporting that the infamous Lockbit ransomware gang is reportedly offline. "

Publicly disclosed U.S. ransomware attacks in 2023 - TechTarget

Source: https://www.techtarget.com/searchsecurity/feature/Publicly-disclosed-US-ransomware-attacks-in-2023

From the Article: "Ransomware attacks continue to plague the U.S., and it's often difficult to gauge just how bad the problem is."

Union Officials Mull Lawsuits After Oakland Ransomware Attack - Government Technology

Source: https://www.govtech.com/security/union-officials-mull-lawsuits-after-oakland-ransomware-attack

From the Article: "Numerous city workers received alerts this month confirming the worst: strangers were attempting to open lines of credit on their accounts, using social security numbers hacked from the city during a ransomware attack that began Feb 8."

Ransomware attacks hit health sector hardest in 2022, FBI says | InsideCyberSecurity.com

Source: https://insidecybersecurity.com/daily-news/ransomware-attacks-hit-health-sector-hardest-2022-fbi-says

From the Article: "Healthcare entities made up the largest share of ransomware attack targets in 2022, according to an FBI report that underlines recent emphasis on the

growth of cyberattacks against critical U.S. infrastructure."

New CISA Program to Warn Critical Infrastructure Companies of Vulnerabilities That Could ...

Source: https://www.cpomagazine.com/cyber-security/new-cisa-program-to-warn-critical-infrastructure-companies-of-vulnerabilities-that-could-invite-ransomware-attacks/

From the Article: "The Cybersecurity and Infrastructure Security Agency (CISA) has announced a proactive new program to keep tabs on potential vulnerabilities in critical infrastructure sector companies, in the interest of curtailing ransomware attacks."

Ransomware attacks up 45% in February, LockBit responsible | Computer Weekly

Source: https://www.computerweekly.com/news/365534069/Ransomware-attacks-up-45-in-February-LockBit-responsible

From the Article: "After a month-on-month decline during the first few weeks of 2023, the number of ransomware attacks tracked in the wild soared by 45% in February, largely driven by an increase in LockBit activity, according to proprietary data published today by NCC Group."

73% of organisations hit by ransomware in 2022 – study | Insurance Business America

Source: https://www.insurancebusinessmag.com/us/news/cyber/73-of-organisations-hit-by-ransomware-in-2022--study-441023.aspx

From the Article: "The survey was conducted by independent research company Vanson Bourne. It polled IT professionals at companies with between 100 and 2,500 employees, across a range of industries and around the globe."

CISA Wants You To Report Anything You Know About Ransomware Activity

Source: https://www.campussafetymagazine.com/public/cisa-wants-you-to-report-anything-you-know-about-ransomware-activity/

From the Article: "The U.S. Cybersecurity and Infrastructure Security Agency (CISA) is

launching its Pre-Ransomware Notification Initiative designed to help organizations thwart ransomware attacks in the early stages of incidents as ransomware actors dwell in a victim's environment before deploying the ransomware."

Experts warn against ransomware complacency - CFO Dive

Source: https://www.cfodive.com/news/experts-warn-against-ransomware-complacency/646114/

From the Article: "Corporate leaders would be mistaken to interpret reports of fewer ransomware-related cyber insurance claims and decelerating premiums in 2022 as evidence of a diminished threat level, according to cybersecurity experts."

38% of organizations hit with ransomware in 2022 were repeat victims - PR Newswire

Source: https://www.prnewswire.com/news-releases/38-of-organizations-hit-with-ransomware-in-2022-were-repeat-victims-301782601.html

From the Article: " Barracuda Networks, Inc., a trusted partner and leading provider of cloud-first security solutions, today published its 2023 Ransomware Insights report, which shows that 73% of the organizations surveyed report being hit with at least one successful ransomware attack in 2022 — and 38% say they were hit twice or more."

Did the Tri Counties Bank Ransomware Attack Leak Customers' Information? - JD Supra

Source: https://www.jdsupra.com/legalnews/did-the-tri-counties-bank-ransomware-5307668/

From the Article: "On March 24, 2023, Tri Counties Bank posted a "Network Outage Update" after determining that a recent ransomware attack may have resulted in confidential consumer data being exposed to hackers."

Research: Risk of Ransomware Attacks in Indonesia Increases - D-Insights

Source: https://dinsights.katadata.co.id/read/2023/03/28/research-risk-of-ransomware-attacks-in-indonesia-increases

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

From the Article: "Cybersecurity company Palo Alto Networks published research findings that stated ransomware cases and extortion through digital platforms in Indonesia increased by 30 percent (year-on-year) in 2022."

City offers employee identity theft protection after ransomware attack | National News - KPVI

Source: https://www.alexcityoutlook.com/news/city-offers-employee-identity-theft-protection-after-ransomware-attack/article_ec35cb92-cb1a-11ed-8cc3-7bd01145027a.html

From the Article: "Alexander City Mayor Woody Baird praised city employees during Monday's council meeting for restoring the city to normal operations following the Jan. 24 ransomware attack. "

The fastest way to recover from ransomware - Robotics & Automation News

Source: https://roboticsandautomationnews.com/2023/03/27/the-fastest-way-to-recover-from-ransomware/66252/

From the Article: "Ransomware file recovery is a delicate process that requires knowledge, experience, and expertise, as one wrong move can result in permanently corrupted data that is impossible to restore."

ISIS Supporter Reports On Ransomware Cyber Attack - MEMRI

Source: https://www.memri.org/cjlab/isis-supporter-reports-vice-society-ransomware-cyber-attack-san-francisco-transit-system

From the Article: "On March 22, 2023, a pro-Islamic Stte (ISIS) channel on the ISIS-operated Rocket.Chat server reported on a recent cyber attack carried out by ransomware group Vice Society which targeted the metro transit system of the San Francisco Bay Area. The post also described previous hacking attacks carried out by the group."

CISA summons outside tips to alert victims of early-stage ransomware | Cybersecurity Dive

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.cybersecuritydive.com/news/cisa-pre-ransomware-notification/646041/

From the Article: "Federal cyber authorities shared early, promising results last week of a pre-ransomware notification initiative designed to quickly alert organizations of intrusions before ransomware actors encrypt or steal data."

Shining Light on Dark Power: Yet Another Ransomware Gang - Trellix

Source: https://www.trellix.com/en-us/about/newsroom/stories/research/shining-light-on-dark-power.html

From the Article: "Another day, another ransomware gang. The Dark Power ransomware gang is new on the block, and is trying to make a name for itself. This blog dives into the specifics of the ransomware used by the gang, as well as some information regarding their victim naming and shaming website, filled with non-paying victims and stolen data."

Threat Detection Series: Watch the PowerShell power hour

Source: https://redcanary.com/blog/threat-detection-series-powershell/

From the Article: "For the fifth year in a row, PowerShell (T1059.001) placed high among the most prevalent ATT&CK techniques ranked in Red Canary's annual Threat Detection Report. Coming in at number 2 this year, PowerShell abuse shows no signs of slowing down, as adversaries find new ways to automate malicious behavior that blends in with normal Windows configurations. "

Live from New York, it's Threat Detection Series Live!

Source: https://redcanary.com/blog/threat-detection-series-event/

From the Article: "Gain additional insights and take home new tools that will help you understand, detect, and emulate the threats in our fifth annual Threat Detection Report."

The Security Vulnerabilities of Message Interoperability

Link back to Table of Contents

Source: https://www.schneier.com/blog/archives/2023/03/the-security-vulnerabilities-of-message-interoperability.html

From the Article: "Interoperability will vastly increase the attack surface at every level in the stack - from the cryptography up through usability to commercial incentives and the opportunities for government interference."

Security Vulnerabilities in Snipping Tools

Source: https://www.schneier.com/blog/archives/2023/03/security-vulnerabilities-in-snipping-tools.html

From the Article: "Both Google's Pixel's Markup Tool and the Windows Snipping Tool have vulnerabilities that allow people to partially recover content that was edited out of images."

Copy-paste heist or clipboard-injector attacks on cryptousers

Source: https://securelist.com/copy-paste-heist-clipboard-injector-targeting-cryptowallets/109186/

From the Article: "It is often the case that something new is just a reincarnation of something old. We have come across a series of clipboard injection attacks on cryptocurrency users, which emerged starting from September 2022. Although we have written about a similar malware attack in 2017 in one of our blogposts, the technique is still very relevant today as it doesn't have any perfect solution from the perspective of operating system design. "

Financial cyberthreats in 2022

Source: https://securelist.com/financial-cyberthreats-in-2022/109219/

From the Article: "Financial gain remains the key driver of cybercriminal activity. In the past year, we've seen multiple developments in this area – from new attack schemes targeting contactless payments to multiple ransomware groups continuing to emerge and haunt businesses."

Link back to Table of Contents

New Mélofée Linux malware linked to Chinese APT groups

Source: https://securityaffairs.com/144210/apt/melofee-malware-linked-to-china.html

From the Article: "Cybersecurity researchers from ExaTrack recently discovered a previously undetected malware family, dubbed Mélofée, targeting Linux servers."

Google TAG shares details about exploit chains used to install commercial spyware

Source: https://securityaffairs.com/144174/hacking/exploit-chains-zero-day-spyware.html

From the Article: "Google's Threat Analysis Group (TAG) discovered several exploit chains targeting Android, iOS, and Chrome to install commercial spyware."

2022 Industry Threat Recap: Finance and Insurance

Source: https://securityintelligence.com/articles/2022-industry-threat-recap-finance-insurance/

From the Article: "The finance and insurance sector proved a top target for cybersecurity threats in 2022. The IBM Security X-Force Threat Intelligence Index 2023 found this sector ranked as the second most attacked, with 18.9% of X-Force incident response cases."

Cyber Storm Predicted at the 2023 World Economic Forum

Source: https://securityintelligence.com/articles/cyber-storm-predicted-at-the-2023-world-economic-forum/

From the Article: "According to the Global Cybersecurity Outlook 2023, 93% of cybersecurity leaders and 86% of business leaders think a far-reaching, catastrophic cyber event is at least somewhat likely in the next two years. Additionally, 43% of organizational leaders think it is likely that a cyberattack will affect their organization severely in the next two years."

Unpatched Security Flaws Expose Water Pump Controllers to Remote Hacker 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.

Source: https://www.securityweek.com/unpatched-security-flaws-expose-water-pump-controllers-to-remote-hacker-attacks/

From the Article: "Water pumping systems made by ProPump and Controls are affected by several vulnerabilities that could allow hackers to cause significant problems."

Microsoft Cloud Vulnerability Led to Bing Search Hijacking, Exposure of Office 365 Data

Source: https://www.securityweek.com/microsoft-cloud-vulnerability-led-to-bing-search-hijacking-exposure-of-office-365-data/

From the Article: "An Azure Active Directory (AAD) misconfiguration leading to Bing.com compromise earned Wiz researchers a $40,000 bug bounty reward."

500k Impacted by Data Breach at Debt Buyer NCB

Source: https://www.securityweek.com/500k-impacted-by-data-breach-at-debt-buyer-ncb/

From the Article: "NCB Management Services is informing roughly 500,000 individuals of a data breach impacting their personal information."

Chinese Cyberspies Use 'Melofee' Linux Malware for Stealthy Attacks

Source: https://www.securityweek.com/chinese-cyberspies-use-melofee-linux-malware-for-stealthy-attacks/

From the Article: "The recently identified Melofee Linux implant allowed Chinese cyberespionage group Winnti to conduct stealthy, targeted attacks."

OpenAI Patches Account Takeover Vulnerabilities in ChatGPT

Source: https://www.securityweek.com/openai-patches-account-takeover-vulnerabilities-in-chatgpt/

From the Article: "OpenAI resolved severe ChatGPT vulnerabilities that could have been exploited to take over accounts."

Link back to Table of Contents

New Wi-Fi Attack Allows Traffic Interception, Security Bypass

Source: https://www.securityweek.com/new-wi-fi-attack-allows-traffic-interception-security-bypass/

From the Article: "A group of academic researchers devised an attack that can intercept Wi-Fi traffic at the MAC layer, bypassing client isolation."

Google Links More iOS, Android Zero-Day Exploits to Spyware Vendors

Source: https://www.securityweek.com/google-links-more-ios-android-zero-day-exploits-to-spyware-vendors/

From the Article: "Google has linked several zero-day vulnerabilities used last year to target Android and iOS devices to commercial spyware vendors."

Most Weaponized Vulnerabilities of 2022 and 5 Key Risks: Report

Source: https://www.securityweek.com/most-weaponized-vulnerabilities-of-2022-and-5-key-risks-report/

From the Article: "A new research report discusses the five most exploited vulnerabilities of 2022, and the five key risks that security teams should consider."

Over 200 Organizations Targeted in Chinese Cyberespionage Campaign

Source: https://www.securityweek.com/over-200-organizations-targeted-in-chinese-cyberespionage-campaign/

From the Article: "Chinese cyberespionage group Mustang Panda was seen targeting maritime, shipping, border control, and immigration organizations in recent attacks."

Microsoft Puts ChatGPT to Work on Automating Cybersecurity

Source: https://www.securityweek.com/microsoft-puts-chatgpt-to-work-on-automating-

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/

From the Article: "Microsoft has rolled out a preview version of Security Copilot, a ChatGPT-powered tool to help organizations automate cybersecurity tasks."

Squeamish over AI. Combosquatting in phishbait. False positives. Cyber phases of the hybrid war. "Credit washing."

Source: https://thecyberwire.com/newsletters/daily-briefing/12/61

From the Article: "An open letter asks for a pause in advanced AI development. All your grammar and usage are belong us. Combosquatting might fool even the wary. Defender had flagged Zoom and other safe sites as dangerous."

New Wi-Fi Protocol Security Flaw Affecting Linux, Android and iOS Devices

Source: https://thehackernews.com/2023/03/new-wi-fi-protocol-security-flaw.html

From the Article: "A group of academics from Northeastern University and KU Leuven has disclosed a fundamental design flaw in the IEEE 802.11 Wi-Fi protocol standard, impacting a wide range of devices running Linux, FreeBSD, Android, and iOS."

AlienFox Malware Targets API Keys and Secrets from AWS, Google, and Microsoft Cloud Services

Source: https://thehackernews.com/2023/03/alienfox-malware-targets-api-keys-and.html

From the Article: "A new "comprehensive toolset" called AlienFox is being distributed on Telegram as a way for threat actors to harvest credentials from API keys and secrets from popular cloud service providers."

Researchers Detail Severe "Super FabriXss" Vulnerability in Microsoft Azure SFX

Source: https://thehackernews.com/2023/03/researchers-detail-severe-super.html

From the Article: "Details have emerged about a now-patched vulnerability in Azure Service Fabric Explorer (SFX) that could lead to unauthenticated remote code

execution."

Chinese RedGolf Group Targeting Windows and Linux Systems with KEYPLUG Backdoor

Source: https://thehackernews.com/2023/03/chinese-redgolf-group-targeting-windows.html

From the Article: "A Chinese state-sponsored threat activity group tracked as RedGolf has been attributed to the use of a custom Windows and Linux backdoor called KEYPLUG. "

Cyberstorage: Leveraging the Multi-Cloud to Combat Data Exfiltration

Source: https://thehackernews.com/2023/03/cyberstorage-leveraging-multi-cloud-to.html

From the Article: "Multi-cloud data storage, once merely a byproduct of the great cloud migration, has now become a strategy for data management. "Multi-cloud by design," and its companion the supercloud, is an ecosystem in which several cloud systems work together to provide many organizational benefits, including increased scale and overall resiliency."

Spyware Vendors Caught Exploiting Zero-Day Vulnerabilities on Android and iOS Devices

Source: https://thehackernews.com/2023/03/spyware-vendors-caught-exploiting-zero.html

From the Article: "A number of zero-day vulnerabilities that were addressed last year were exploited by commercial spyware vendors to target Android and iOS devices, Google's Threat Analysis Group (TAG) has revealed."

Mélofée: Researchers Uncover New Linux Malware Linked to Chinese APT Groups

Source: https://thehackernews.com/2023/03/melofee-researchers-uncover-new-linux.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: "An unknown Chinese state-sponsored hacking group has been linked to a novel piece of malware aimed at Linux servers."

Microsoft Defender shoots down legit URLs as malicious

Source: https://www.theregister.com/2023/03/29/microsoft_defender_url_alerts/

From the Article: "Updated Microsoft's at-times-glitchy Defender service is again causing headaches for IT admins by flagging legitimate URLs as malicious."

DDoS DNS attacks are old-school, unsophisticated … and they're back

Source: https://www.theregister.com/2023/03/29/ddos_dns_attacks_are_oldschool/

From the Article: "Ransomware may currently be the biggest bogeyman for cybersecurity pros, law enforcement, and governments, but it shouldn't divert us from more traditional, but still very disruptive threats."

3 Shifts in the Cyber Threat Landscape

Source: https://www.trendmicro.com/en_us/ciso/23/c/cyber-threat-landscape-2023.html

From the Article: "The threat landscape is always changing and these three major shifts are already underway. Learn to recognize them to protect your organization from cyber threats."

New OpcJacker Malware Distributed via Fake VPN Malvertising

Source: https://www.trendmicro.com/en_us/research/23/c/new-opcjacker-malware-distributed-via-fake-vpn-malvertising.html

From the Article: "We discovered a new malware, which we named "OpcJacker" (due to its opcode configuration design and its cryptocurrency hijacking ability), that has been distributed in the wild since the second half of 2022."

Link back to Table of Contents

Squeezing Secrets Out Of An Amazon Echo Dot

Source: https://hackaday.com/2023/04/01/squeezing-secrets-out-of-an-amazon-echo-dot/

From the Article: "As we have seen time and time again, not every device stores our sensitive data in a respectful manner. Some of them send our personal data out to third parties, even! Today's case is not a mythical one, however — it's a jellybean Amazon Echo Dot, and [Daniel B] shows how to make it spill your WiFi secrets with a bit of a hardware nudge."

Elbridge Colby: China is more dangerous than Russia

Source: https://unherd.com/2023/04/elbridge-colby-china-is-more-dangerous-than-russia/

From the Article: "Donald Trump's foreign policy advisor warns of a new Cold War"

Intel announces rival chip processing plant to be built in michigan afd2023

Source: https://columbusunderground.com/intel-announces-rival-chip-processing-plant-to-be-built-in-michigan-afd2023/

From the Article: "On the heels of its recent groundbreaking for a new semiconductor factory complex being built in Central Ohio, Intel has made yet another surprising announcement — it will also build a rival chip processing plant in Michigan."

German researchers devise method to detect manipulations in chips

Source: https://www.allaboutcircuits.com/news/german-researchers-devise-method-to-detect-manipulations-in-chips/

From the Article: "German researchers developed a new method to detect hardware manipulations in microchips early on in the production process—a time when chips are most vulnerable."

Samsung to build £189.6bn semiconductor 'mega cluster'

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://eandt.theiet.org/content/articles/2023/03/samsung-to-build-1896bn-semiconductor-mega-cluster/

From the Article: "Samsung Electronics plans to build the “world’s largest” semiconductor manufacturing base in Seoul, South Korea. The South Korea-based chipmaker expects to invest 300 trillion won (£189bn) over the next 20 years to build five chipmaking plants near Seoul. "

Samsung considers chip packaging test line in Japan as it seeks deeper cooperation - sources

Source: https://finance.yahoo.com/news/samsung-considering-chip-test-line-080902071.html

From the Article: "TOKYO/SEOUL (Reuters) -South Korea's Samsung Electronics Co Ltd is considering setting up a chip packaging test line in Japan, five people said, to bolster its advanced packaging business and forge closer ties with Japanese makers of semiconductor equipment and materials."

Cryptocurrencies add nothing useful to society, says chip-maker Nvidia

Source: https://www.theguardian.com/technology/2023/mar/26/cryptocurrencies-add-nothing-useful-to-society-nvidia-chatbots-processing-crypto-mining

From the Article: "Tech chief says the development of chatbots is a more worthwhile use of processing power than crypto mining"

Japan joins in on chip sanctions against China

Source: https://evertiq.com/design/53523

From the Article: "Japan will impose export restrictions on a variety of semiconductor manufacturing tools, aligning its technology trade restrictions with US efforts to limit China's capacity to produce cutting-edge chips."

Multi-die systems define the future of semiconductors

Link back to Table of Contents

Source: https://www.technologyreview.com/2023/03/31/1070527/multi-die-systems-define-the-future-of-semiconductors/

From the Article: "Multi-die system or chiplet-based technology is a big bet on high-performance chip design—and a complex challenge."

Micron sees fab capacity utilization hit record low

Source: https://www.digitimes.com/news/a20230330PD205/memory-chips-micron-technology-utilization-rate.html

From the Article: "Micron Technology's memory wafer fab capacity utilization is now at a record low level, the company confirmed at its latest earnings call conference. The company didn't release the utilization figure, nor did it predict when its capacity will be fully..."

Nexperia argues forced sale would close Newport fab

Source: https://www.eenewseurope.com/en/nexperia-argues-forced-sale-would-close-newport-fab/

From the Article: "In November 2022 the UK government told Nexperia it must reduce its ownership of the Welsh wafer fab to less than 14 percent on the grounds of national security. Early in 2023 Nexperia said it would seek a judicial review with the High Court (see Nexperia lawyers up for fight over Newport Wafer Fab)."

Foundry Sales Exceed NAND, Approach DRAM at Samsung Electronics

Source: http://www.businesskorea.co.kr/news/articleView.html?idxno=111200

From the Article: "Samsung Electronics' foundry business sales hit 7,016.4 billion won (US$5.391 billion) in the fourth quarter of last year, said market research firm TrendForce on March 19. Compared to DRAM sales of 7,210.3 billion won, or US$5.54 billion, the gap was less than 200 billion won."

TSMC may not expand in US if double taxation rule continues | AppleInsider

Link back to Table of Contents

Source: https://appleinsider.com/articles/23/03/30/tsmc-may-not-expand-in-us-if-double-taxation-rule-continues

From the Article: "According to the Financial Times, unless there is a change in the law, TSMC will be paying out over 50% of its profits earned in the US. In comparison, Samsung pays much less because its home country of South Korea has a tax treaty with the States. Naturally, then, US politicians who want to see the firm expand in the States argue that President Biden should negotiate a tax accord with Taiwan."

Ford's new Tennessee plant aims to build 500,000 electric trucks a year

Source: https://www.reuters.com/business/autos-transportation/fords-new-tennessee-plant-aims-build-500000-electric-trucks-year-2023-03-24/

From the Article: "STANTON, Tennessee, March 24 (Reuters) - Ford Motor Co (F.N) plans to build up to 500,000 electric trucks a year at its BlueOval City complex under construction in western Tennessee, the automaker said on Friday."

Public opinion on the island questioned the harsh terms of the U.S. Chip Act, worrying that TSMC would be "killed" by the U.S.

Source: https://www.linkedin.com/pulse/public-opinion-island-questioned-harsh-terms-us-chip-act-anne-ren/

From the Article: "The U.S. "Chip and Science Act" will open applications for subsidies for semiconductor companies setting up factories in the United States. Some of the harsh clauses have caused public opinion on the island to sweat for TSMC."

Whatever happened to the global chip shortage?

Source: https://www.foxnews.com/politics/whatever-happened-global-chip-shortage

From the Article: "Bret Baier looks at where semiconductor manufacturing is on the rise and how soon US will be able to compete globally"

'We are not ready': An interview with Taiwan's former military chief

Link back to Table of Contents

Source: https://www.japantimes.co.jp/news/2023/03/30/asia-pacific/taiwan-lee-hsi-min-interview-transcript/

From the Article: "While Beijing has repeatedly stated that it seeks unification through peaceful means, it has also refused to rule out the use of force, prompting the democratic island to further ramp up its defenses and strengthen relations with friendly countries, particularly the United States."

Chip Industry's Technical Paper Roundup: Mar. 28

Source: https://semiengineering.com/chip-industrys-technical-paper-roundup-mar-28/

From the Article: "GAA FETs; thermal simulation in 3D-IC; zero trust environments; silicon photonics MEMS; semi-metals for interconnects; logic locking at the RTL; mechanical overtone frequency combs; photonics: GaSb/SiN tunable hybrid integrated laser; domain wall-magnetic tunnel junction analog content addressable memory."

Hackers probing contractors for path to Pentagon, DISA chief says

Source: https://www.c4isrnet.com/industry/2023/03/30/hackers-probing-contractors-for-path-to-pentagon-disa-chief-says/

From the Article: "WASHINGTON — Foreign hackers are targeting contractors to the U.S. government not only for their intellectual property and non-public information, but also to find furtive avenues into Pentagon networks, according to the director of the Defense Information Systems Agency."

Supply shortages threaten U.S. infrastructure and war efforts

Source: https://www.reuters.com/business/ongoing-supply-shortages-threaten-us-infrastructure-war-efforts-2023-03-29/

From the Article: "Companies that make war weapons like shoulder-fired Javelin and Stinger missiles are awaiting U.S. funding before starting new production for Ukraine. When the defense industry gets that greenlight, their scramble to source semiconductors and other hard-to-find electronic components could usher in a new wave of supply chain snarls that disrupt production and drive up costs."

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 U.S. Department of State International Technology Security and Innovation Fund - United States Department of State

Source: https://www.state.gov/the-u-s-department-of-state-international-technology-security-and-innovation-fund/

From the Article: "The International Technology Security and Innovation (ITSI) Fund, appropriated under the Creating Helpful Incentives to Produce Semiconductors (CHIPS) Act of 2022, provides the Department of State with $500 million — $100 million per year over five years, starting in Fiscal Year 2023 — to promote the development and adoption of secure and trustworthy telecommunications networks and ensure semiconductor supply chain security and diversification."

Greater ownership is the key to bridging the Valley of Death

Source: https://defensescoop.com/2023/03/20/greater-ownership-is-the-key-to-bridging-the-valley-of-death/

From the Article: "Historically, culture in government has led to maintaining the status quo. However, to successfully bring new tech into government, Okano emphasizes the need for collaboration across different departments. “The organizations that do well that we’ve seen at transitioning technology have really solid relationships with the organizations that do a lot of the S&T work,” Okano explained."

Italy curbs ChatGPT, starts probe over privacy concerns

Source: https://www.reuters.com/technology/italy-data-protection-agency-opens-chatgpt-probe-privacy-concerns-2023-03-31/

From the Article: "MILAN/STOCKHOLM, March 31 (Reuters) - OpenAI has taken ChatGPT offline in Italy after the government's Data Protection Authority on Friday temporarily banned the chatbot and launched a probe over the artificial intelligence application's suspected breach of privacy rules."

Using IC Programming, Provisioning for Device Security - EE Times

Source: https://www.eetimes.com/using-ic-programming-provisioning-for-device-security/

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: "With billions of devices connected to cloud applications and services, secure programming and provisioning of integrated circuits form the foundation for protecting chips. The journey to understand the security challenges related to IC programming and provisioning begins with some definitions."

Biden invokes Defense Production Act for printed circuit board production

Source: https://www.reuters.com/world/us/biden-invokes-defense-production-act-printed-circuit-board-production-2023-03-27/

From the Article: "WASHINGTON, March 27 (Reuters) - U.S. President Joe Biden on Monday invoked the Defense Production Act to spend $50 million on domestic and Canadian production of printed circuit boards, citing the technology's importance to national defense."

Order cutbacks still cast shadow over TSMC revenue prospects

Source: https://www.digitimes.com/news/a20230330PD215/apple-chatgpt-ic-manufacturing-nvidia-tsmc.html

From the Article: "TSMC continues to experience cutbacks in orders from major customers including MediaTek and Apple, according to industry sources. Besides, the foundry has yet to ramp up wafer starts for Nvidia's chips, which enable ChatGPT and other large language..."

Chinese fabless chip design sector remains small despite increasing R&D efforts

Source: https://www.digitimes.com/news/a20230331VL206/china.html

From the Article: "As DIGITIMES Research estimates, the United States retains the most competent IC design industry, aided by a complete scientific research ecosystem, the CHIPS Act, and the sanctions against China's HPC industry."

Packaging substrate demand remains promising

Source: https://www.digitimes.com/news/a20230330PD211/hpc-ic-manufacturing-packaging-substrate-tsmc.html

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

From the Article: "The outlook of mid- to long-term demand for substrates supporting the packaging of HPC chips remains bright despite recent speculation that the market for related substrates is oversupplied."

Hua Hong saw sales grow by 51% in 2022, may increase CAPEX despite downturn

Source: https://www.digitimes.com/news/a20230331VL203/china-hua-hong-semiconductor-ic-manufacturing.html

From the Article: "Hua Hong Semiconductors posted an annual growth of 51.8% in sales in 2022, a record high for the second-largest pure-play foundry in China. The company committed to increasing capital expenditure despite a downturn seen in the chip industry."

Japan tightens chip gear exports as US seeks to contain China

Source: https://www.digitimes.com/news/a20230331VL207/china-exports-ic-manufacturing-japan-us.html

From the Article: "Japan said it will expand restrictions on exports of 23 types of leading-edge chipmaking technology, as the US ratchets up efforts to limit China's access to key semiconductor knowhow."

Samsung said to directly develop 8-inch process for GaN, SiC devices

Source: https://www.digitimes.com/news/a20230331PD202/8-inch-fab-gan-ic-manufacturing-samsung-sic.html

From the Article: "Samsung Electronics reportedly will directly migrate to 8-inch process for third-generation semiconductors SiC and GaN devices now under development by its power semiconductor task force set up in early 2023."

IDMs upbeat about revenue prospects, benefiting Taiwan supply chain partners

Source: https://www.digitimes.com/news/a20230331PD201/ic-manufacturing-igbt-industrial-control-power-semiconductors.html

Link back to Table of Contents

From the Article: "Robust demand for Si-IGBT and SiC power modules for automotive and industrial control applications has inspired IDMs such as Infineon to become upbeat about their revenue prospects for 2023, which is expected to benefit their manufacturing partners..."

Ford joins a US$4.51 billion nickel processing project in Indonesia

Source: https://www.digitimes.com/news/a20230331VL205/battery+green-energy-china-ford-motor-indonesia-nickel.html&chid=10

From the Article: "US automaker Ford made a battery material investment in Indonesia, a first for the company in Southeast Asia. The US$4.51 billion project is also joined by PT Vale Indonesia and Huayou Cobalt, targeting 120 kilotons of mixed hydroxide precipitate (MHP)..."

With 3D processing speeds 900 times faster than GPUs, AI semiconductors assist the metaverse

Source: https://www.digitimes.com/news/a20230331PD204/ai-image-rendering-metaverse-south-korea.html

From the Article: "Recently, a South Korean research team successfully developed an AI semiconductor that can be used in mobile devices and can increase speed and energy efficiency. This result is anticipated to become the basis for increasing the completeness and spread..."

NXP supportive of semiconductor manufacturing ecosystem in India

Source: https://www.digitimes.com/news/a20230331VL200/ic-manufacturing-india-nxp-semiconductor.html

From the Article: "Netherlands-based NXP is looking to support a rapidly developing electronics manufacturing ecosystem in India by encouraging semiconductor manufacturers to invest in the nation."

India's 5G deployment speeds up, on way to reach full coverage by 2024

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.digitimes.com/news/a20230331VL201/5g-india-mobile+telecom.html

From the Article: "Thanks to strong government support for digital transformation, telecom operators' aggressive deployment of 5G infrastructure, and more affordable 5G smartphones, India has seen its number of 5G base transceiver stations rise faster."

Micron cements market share with enhanced NAND portfolio

Source: https://www.digitimes.com/news/a20230330PD201/dram-micron-technology-nand.html

From the Article: "US memory maker Micron Technology has given a positive outlook for the third quarter of fiscal 2023 (March-May), expecting its DRAM sales to grow slightly in the quarter and NAND shipments to surge significantly, as customer inventories are getting..."

SMIC weighed down by talent shortage and reliance on mature nodes

Source: https://www.digitimes.com/news/a20230331PD205/28nm-china-smic.html

From the Article: "Following two years of US sanctions, Chinese foundry champion Semiconductor Manufacturing International Corp. (SMIC) has been focusing on legacy process nodes like 28nm. According to the Chinese foundry, 28nm is the node favored by SMIC customers in applications like consumer electronics, Internet of Things (IoT) and automotive electronics."

Taiwan's automotive supply chain remains stable amid Chinese market's chaos and rapid changes

Source: https://www.digitimes.com/news/a20230329PD204/automotive-supply-chain-china-green-energy.html

From the Article: "China's car market has been caught up in a frenzy of price cuts recently due to Tesla's significant price reduction after localizing its production in China, making it the US leading new energy vehicle (NEV) manufacturer. Tesla's successive price reductions..."

Link back to Table of Contents

AI spending in Asia Pacific to reach US$49 billion by 2026 despite current economic challenges, says IDC

Source: https://www.digitimes.com/news/a20230329PR200/ai-asia-pacific-software-big-data.html

From the Article: "According to IDC's latest Worldwide Artificial Intelligence Spending Guide, spending in the Asia Pacific on Artificial Intelligence (AI), including software, services, and hardware for AI-centric systems, will grow to US$49.2 billion in 2026, with a..."

GMI upbeat about chip demand for automotive, broadband, and wearable apps

Source: https://www.digitimes.com/news/a20230330PD208/demand-ic-design-distribution-inventory-pc-ce-wearable.html

From the Article: "IC distributor GMI Technology expects its customers to start replenishing inventory in the second half of 2023, while eyeing a pick-up in demand from the persistently expanding automotive, broadband, and wearable device markets."

ITE Tech sees PC customers start replenishing inventory

Source: https://www.digitimes.com/news/a20230330PD210/ic-design-inventory-ite-tech-ite-notebook-demand.html

From the Article: "Taiwan-based IC design house ITE Tech said its PC customers are starting to replenish inventory, especially inventory for Chromebook and gaming models."

Taiwan passive component makers look to high-margin offerings for growth

Source: https://www.digitimes.com/news/a20230330PD207/ever-ohms-passive-component-passive-pcb-other-ic-components.html

From the Article: "Automotive and other high-margin products will be critical in boosting sales at Taiwan-based passive component suppliers in 2023, according to industry 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.

Tougher US ban may alter China IC manufacturing ecosystem, says TSMC chair

Source: https://www.digitimes.com/news/a20230330PD206/ic-manufacturing-semiconductor-industry-taiwan-semiconductor-industry-association-taiwan-tsia-tsmc.html

From the Article: "Tougher semiconductor-related export bans by the US may impact China's IC manufacturing ecosystem in the future, said Mark Liu, chairman of TSMC."

Chinese IC design industry leaders weigh options after US sanctions

Source: https://www.digitimes.com/news/a20230330VL210/china-ic-design-distribution.html

From the Article: "At the annual China IC Leadership Summit held on March 30, Wayne Dai, founder and CEO of Chinese IC design house VeriSilicon, observed that chiplet development in China is basically underpinned by three process nodes: 28/22nm, 14/12nm and 5nm, as reported..."

GlobalWafers remains upbeat about 3rd-gen semiconductor demand

Source: https://www.digitimes.com/news/a20230330PD212/auto-components-chips+components-globalwafers-ic-manufacturing-tesla.html

From the Article: "The outlook for third-generation semiconductor demand remains positive, according to GlobalWafers chairperson Doris Hsu, who was speaking in the wake of Tesla's intention to slash its use of SiC components in EVs."

Solomon Systech launches PM microLED DDI

Source: https://www.digitimes.com/news/a20230330VL207.html

From the Article: "Solomon Systech, which specializes in the design and development of proprietary display IC products and system solutions, has announced the release of what the company claims is the world's first PM-MicroLED display driver. The new SSD2363 enables the..."

Link back to Table of Contents

Taiwan bond 'unbreakable': Guatemala - Taipei Times

Source: https://www.taipeitimes.com/News/front/archives/2023/04/02/2003797165

From the Article: "Guatemala on Friday said its ties with Taiwan are firm, reiterating support for its Asian ally just a week after neighboring Honduras cut its ties with Taipei in favor of China."

Beijing eroding the independence of HK courts: Blinken - Taipei Times

Source: https://www.taipeitimes.com/News/front/archives/2023/04/02/2003797168

From the Article: "US Secretary of State Antony Blinken on Friday accused China of undermining the independence of Hong Kong's courts, as the US Department of State released a report condemning Beijing's crackdown on dissent in the territory."

'Breakthrough' in Taiwan relations: Canadian report - Taipei Times

Source: https://www.taipeitimes.com/News/front/archives/2023/04/01/2003797112

From the Article: "The Special Committee on Canada-China Relations in the Canadian House of Commons on Thursday published its first report on Taiwan, which analysts in Taiwan have called a "breakthrough" in bilateral relations."

French documentary focuses on Taiwanese identity - Taipei Times

Source: https://www.taipeitimes.com/News/taiwan/archives/2023/04/02/2003797178

From the Article: "The law and diplomacy are not on Taiwan's side, given that the legal principles and diplomatic frameworks regarding Taiwan were set 50 years ago, when it was under martial law and the people did not have a voice, he said. That meant the "one China" concept, in which Taiwan is seen as a part of China, was formed without asking for the opinion of Taiwanese, he said."

Nous sommes Taïwan - Regarder le documentaire complet | ARTE

Source: https://www.arte.tv/fr/videos/111082-000-A/nous-sommes-taiwan/

Link back to Table of Contents

From the Article: "Video. Four centuries of various subordinations have given the Taiwanese people a pronounced taste for freedom, which remains alive despite Chinese appetites. A look back at the history and specificities of the "beautiful island" by journalist Pierre Haski."

US' top indices rally on inflation data - Taipei Times

Source: https://www.taipeitimes.com/News/biz/archives/2023/04/02/2003797150

From the Article: "CHIPPING IN: Semiconductors were among the quarter's best-performing stocks, with the Philadelphia semiconductor index rising 27.6 percent, as big tech shares also gained"

Gudeng benefiting from US-China tech tensions - Taipei Times

Source: https://www.taipeitimes.com/News/biz/archives/2023/04/01/2003797091

From the Article: "SUBSTITUTE: With the US restricting Chinese access to key components, many Chinese firms have turned to the Taiwanese company for supplies of wafer pods"

TSMC chairman urges government chip initiative - Taipei Times

Source: https://www.taipeitimes.com/News/front/archives/2023/03/31/2003797052

From the Article: "Taiwan Semiconductor Manufacturing Co (TSMC, 台積電) yesterday called on the government to provide more equipment essential to advanced chipmaking, as it seeks to shore up its critical role in a US$550 billion industry."

US sees Taiwan as a global partner: AIT - Taipei Times

Source: https://www.taipeitimes.com/News/front/archives/2023/03/31/2003797050

From the Article: "The US is working with all of its partners, including Taiwan, to uphold key principles of democracy, American Institute in Taiwan Chair Laura Rosenberger said on Wednesday as she hosted President Tsai Ing-wen (蔡英文) in New York."

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 Korean chips bill approved by parliament - Taipei Times

Source: https://www.taipeitimes.com/News/biz/archives/2023/03/31/2003797030

From the Article: "RACE WITH TAIWAN: With the new bill and subsidies, Seoul is hoping to maintain its tech leadership or even supercede Taiwan in the production of logic chips"

Joe Biden warns of potential technology surrender to China - Taipei Times

Source: https://www.taipeitimes.com/News/front/archives/2023/03/30/2003796986

From the Article: "Republicans' ideas for cutting the US budget could undermine manufacturing and help China dominate the world economy, US President Joe Biden said on Tuesday. Speaking at a semiconductor maker in North Carolina to highlight his own policies, Biden is trying to shape public sentiment as he faces off with US House of Representatives Speaker Kevin McCarthy about whether the federal government should increase its borrowing capacity."

China seeks chip talent solutions - Taipei Times

Source: https://www.taipeitimes.com/News/biz/archives/2023/03/30/2003796962

From the Article: "China is ramping up efforts to develop homegrown semiconductor talent as it seeks to rapidly fill a shortage of expertise that has been worsened by US efforts to limit Beijing's access to advanced chip technology. Enrollments for undergraduate and post-graduate courses have surged over the past five years thanks to new funds for top universities as well as a boom in smaller private schools focused on shorter-term instruction."

'Taiwan must improve chip strategy' - Taipei Times

Source: https://www.taipeitimes.com/News/biz/archives/2023/03/29/2003796886

From the Article: "MediaTek Inc (聯發科) chairman Rick Tsai (蔡明介) yesterday urged the government to formulate a state semiconductor strategy and comprehensive "chip

act" that includes local chip designers and smaller-scale semiconductor companies, as they are facing intensifying competition from China."

S Korean envoy aims to boost chip cooperation - Taipei Times

Source: https://www.taipeitimes.com/News/taiwan/archives/2023/03/28/2003796859

From the Article: "South Korean Representative to Taiwan Lee Eun-ho wants to facilitate closer bilateral semiconductor cooperation to improve global supply chain resilience, and believes that his background in engineering can help in that effort, he said in an interview with Taiwanese media."

TSMC wins approval to invest US$3.5bn in Arizona - Taipei Times

Source: https://www.taipeitimes.com/News/biz/archives/2023/03/28/2003796823

From the Article: "The Investment Commission yesterday approved a Taiwan Semiconductor Manufacturing Co (TSMC, 台積電) application to invest an additional US$3.5 billion in its Arizona subsidiary to manufactured advanced chips."

Taiwan seeking to bolster trade with Czech Republic - Taipei Times

Source: https://www.taipeitimes.com/News/biz/archives/2023/03/28/2003796821

From the Article: "Taiwan is seeking to boost bilateral trade cooperation with the Czech Republic, targeting semiconductors, information and communication technology and electric vehicles (EVs), Minister of Economic Affairs Wang Mei-hua (王美花) said yesterday."

Business climate monitor still in 'blue' - Taipei Times

Source: https://www.taipeitimes.com/News/biz/archives/2023/03/28/2003796819

From the Article: "The government's business climate monitor last month signaled "blue" for the fourth consecutive month, indicating a recession, as global inflation and monetary tightening continued to constrain exports and other key economic barometers, the National Development Council said yesterday."

Link back to Table of Contents

Notes from Central Taiwan: 2024 election: same as it ever was - Taipei Times

Source: https://www.taipeitimes.com/News/feat/archives/2023/03/27/2003796785

From the Article: "The list of critical issues the DPP and KMT could run on in next year's election are endless, but count on the focus being China at the expense of everything else"

China hits back at US in chip war with probe into Micron's products

Source: https://www.scmp.com/tech/tech-war/article/3215622/tech-war-china-hits-back-american-chip-firms-regulator-launches-cybersecurity-probe-microns-products

From the Article: "It is the first time that the Chinese government has targeted a US semiconductor company Micron has previously warned investors of the risks of being excluded from the China market"

Japan restricts chipmaking gear exports as US seeks to contain China

Source: https://www.scmp.com/news/asia/east-asia/article/3215505/japan-restricts-chipmaking-equipment-exports-us-seeks-contain-china

From the Article: "The government will impose export controls on 23 types of leading-edge technology used to transform silicon into chips. The move follows months of lobbying by the US to get Tokyo to join it in tightening shipments of semiconductor tools to Beijing."

South Korea cuts chip production most since global financial crisis as demand cools

Source: https://www.scmp.com/tech/tech-trends/article/3215500/south-korea-cuts-chip-production-most-global-financial-crisis-demand-cools

From the Article: "Production dropped 41.8 per cent from a year earlier, worsening from a 33.9 per cent fall in January, according to the national statistics office. Chip makers are important constituents of Korea's trade-reliant economy, accounting for about 12 per cent of the total exports in February."

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.

ASML CEO's China visit unlikely to bear immediate fruit as politics dominate

Source: https://www.scmp.com/tech/tech-war/article/3215441/asml-ceos-china-visit-unlikely-give-immediate-relief-countrys-embattled-chip-sector-geopolitical

From the Article: "ASML CEO Peter Wennink met with China's commerce minister Wang Wentao on Tuesday. The Netherlands is currently mulling further restrictions on exports of chip technology to China."

Chinese foundry SMIC posts record revenue, profits for 2022 despite US sanctions

Source: https://www.scmp.com/tech/big-tech/article/3215254/chinas-top-chip-foundry-smic-posts-record-revenue-profits-2022-despite-us-sanctions

From the Article: "SMIC's revenue grew 33.6 per cent year on year to US$7.2 billion in 2022, while net profits reached US$1.8 billion, both record amounts. R&D spending equalled 10.1 per cent of total revenue, down for a third year from 11.7 per cent and 17.3 per cent in 2021 and 2020, respectively."

China's chip industry faces threats, but not only from the US

Source: https://www.scmp.com/comment/opinion/article/3214995/if-us-doesnt-thwart-chinas-efforts-be-semiconductor-self-sufficient-climate-change-might

From the Article: "As China rushes to build up its chip manufacturing capabilities, climate change is making parts of the country increasingly prone to extreme weather that could create resource scarcities and disrupt operations"

Nvidia shows new research on using AI to improve chip designs

Source: https://www.scmp.com/tech/tech-trends/article/3215068/nvidia-shows-new-research-using-ai-improve-chip-designs

From the Article: "Nvidia released a paper showing that it could use a combination of AI techniques to find better ways to place big groups of transistors to create working chips. The research took an existing effort by the University of Texas, using what is called

Link back to Table of Contents

reinforcement learning, and added a second layer of AI on top for better results."

Why South Koreans are no longer called 'unpatriotic' for buying Japanese goods

Source: https://www.scmp.com/week-asia/politics/article/3215000/japans-uniqlo-asahi-and-lexus-brands-profit-warmer-ties-south-korea

From the Article: "Japanese brands, Uniqlo, Asahi, and Lexus reported a recent surge in sales in South Korea, following a shift in political ties between Tokyo and Seoul. Relations sank to new lows in 2019 after Tokyo placed export controls on South Korea's semiconductor sector, leading to a boycott of Japanese goods."

China's military urged to focus on defence in fighting 'people's war'

Source: https://www.scmp.com/news/china/military/article/3215616/chinas-military-urged-keep-focus-active-defence-fighting-peoples-war

From the Article: "Opinion piece in PLA newspaper could offer hints on the latest thinking about strategy and how Beijing would approach conflict with US or Taiwan. It says that in general the military should 'not aim to achieve hegemony and aggression' as part of its strategy to rally popular support."

China wants closer ties with South Korea, but can politics be set aside?

Source: https://www.scmp.com/news/china/diplomacy/article/3215732/china-wants-warmer-cultural-ties-south-korea-politics-seen-stand-way

From the Article: "Lin Songtian, head of the Chinese People's Association for Friendship with Foreign Countries, speaks of 'shared interest and destiny'. Chinese studies professor in Seoul voices scepticism, as 'people-to-people diplomacy is dictated by politics' under President Xi Jinping."

Why are India and the US signing an MoU on semiconductors?

Source: https://techwireasia.com/2023/03/why-are-india-and-the-us-signing-an-mou-on-semiconductors/

Link back to Table of Contents

From the Article: "The US Commerce Secretary, Gina Raimondo, said that the India-US Memorandum of Understanding (MoU) would significantly help India diversify supply chains. Raimondo and Indian External Affairs Minister, S Jaishankar, also launched a new initiative called the India-US Strategic Trade Dialogue, which will focus on aligning the export control regimes of both countries for critical technologies."

IoT Security: Exploring Risks and Countermeasures Across Industries

Source: https://www.design-reuse.com/articles/53647/iot-security-exploring-risks-and-countermeasures-across-industries.html

From the Article: "The security concern was also highlighted in CNBC's article which says," According to cybersecurity specialists, the swift expansion of IoT (Internet of Things) gadgets in 2022 may have signaled a turning point. Hackers can exploit cars and medical devices, which are essential to daily life and have security vulnerabilities.""

China's reliance on chemical in chip-making process rings alarm bells

Source: https://www.scmp.com/tech/big-tech/article/3212982/tech-war-china-reliance-chemical-chip-manufacturing-causes-ripples-japan-mulls-how-respond-updated

From the Article: "Chinese investors have been scrambling to buy companies that are able, or have the potential, to produce photoresist. Tokyo has yet to make a decision on restricting photoresist sales to China but some investors are already positioning for this outcome."

China's flagship CPU designer puts on a brave face amid US sanctions

Source: https://www.scmp.com/tech/tech-war/article/3213889/tech-war-chinas-flagship-cpu-designer-loongson-puts-brave-face-amid-us-sanctions

From the Article: "Loongson said it is evaluating the advanced 7-nm process from a number of foundries to manufacture its future chips, which include GPUs. The company launched its home-grown 3A5000 CPU at the end of 2020, which was made on a now-restricted process node of 14-nm."

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

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

From the Article: "The Biden administration needs to foster greater public-private collaboration, involve global partners and help build the cyber workforce to fight growing digital threats. "

China's Hidden Tech Revolution

Source: https://www.foreignaffairs.com/china/chinas-hidden-tech-revolution-how-beijing-threatens-us-dominance-dan-wang

From the Article: "How Beijing Threatens U.S. Dominance"

India-US chip partnership could boost global chip supply chain

Source: https://www.computerworld.com/article/3691108/india-us-chip-partnership-could-boost-global-chip-supply-chain.html

From the Article: "India and the US aim to collaboratively build a resilient semiconductor supply chain that is currently in a state of turmoil due to geopolitical disruptions."

How the Dutch turned on Chinese tech

Source: https://www.politico.eu/article/chips-netherlands-mark-rutte-china/

From the Article: "As China shoots for tech supremacy, the Netherlands sides with U.S. to push back."

Georgia Tech and GlobalFoundries to Collaborate on Joint Semiconductor Research and Workforce Development | GlobalFoundries

Source: https://gf.com/gf-press-release/georgia-tech-and-globalfoundries-to-collaborate-on-joint-semiconductor-research-and-workforce-development/

From the Article: "New partnership to include educational opportunities for Georgia Tech students and faculty, STEM outreach, and joint R&D programs on GF technology"

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.

Northern norway fights title world jamming capital dana a goward trackingId LRv9ezwtLrSlBrYqeMntYw 3D 3D

Source: https://www.linkedin.com/pulse/northern-norway-fights-title-world-jamming-capital-dana-a-goward/

From the Article: "Northern Norway seems to be a hotbed of GNSS jamming. We have seen regular reports of interference from Russia across the border. Yesterday the folks at GPSPatron reported more jamming there again."

Supply Chain Weekly Wrap-Up 03/24/2023-03/30/2023

Source: https://www.allthingssupplychain.com/supply-chain-weekly-wrap-up-03-24-2023-03-30-2023/

From the Article: "On Wednesday a part of the Gulf of Mexico, the size of Italy, was put for auction to sell the oil and gas drilling rights. the area auctioned is 73.3 million acres, was made available to drilling companies, less than a month. The sale, known as lease 259, has the potential to extract more than 1 billion barrels of oil. "

We're Good at Finding Security Flaws, But What About Fixing Them?

Source: https://www.veracode.com/blog/secure-development/were-good-finding-security-flaws-what-about-fixing-them

From the Article: "Technology is a double-edged sword. On one hand, it can make new experiences possible and elevate productivity. On the other hand, it introduces new threats and attack vectors; and it can widen the gap even further between our ability to produce software and our ability to secure it. "

The National Intelligence Center of Spain and AWS collaborate to promote public sector cybersecurity

Source: https://aws.amazon.com/blogs/security/the-national-intelligence-center-of-spain-and-aws-collaborate-to-promote-public-sector-cybersecurity/

From the Article: "The National Intelligence Center and National Cryptological Center

Link back to Table of Contents

(CNI-CCN)—attached to the Spanish Ministry of Defense—and Amazon Web Services (AWS) have signed a strategic collaboration agreement to jointly promote cybersecurity and innovation in the public sector through AWS Cloud technology."

The Rise and Fall of Sabu: From Hacker Hero to FBI Informant

Source: https://www.blackhatethicalhacking.com/articles/the-rise-and-fall-of-sabu-from-hacker-hero-to-fbi-informant/

From the Article: "Hector Xavier Monsegur, also known as Sabu, was a prominent member of the hacking collective LulzSec, which gained notoriety in 2011 for a series of high-profile cyber-attacks on government agencies and major corporations."

Microsoft's Misconfigured Application Allowed for Real-Time Breach Attempts on Bing.com

Source: https://www.blackhatethicalhacking.com/news/microsofts-misconfigured-application-allowed-for-real-time-breach-attempts-on-bing-com/

From the Article: "Microsoft has fixed a security flaw that could have allowed malicious actors to modify Bing.com search results and potentially breach the accounts of Office 365 users. The flaw was discovered by Wiz Research, which dubbed the attack "BingBang.""

Threat Roundup for March 24 to March 31

Source: https://blog.talosintelligence.com/threat-roundup-0324-0331-2/

From the Article: "Today, Talos is publishing a glimpse into the most prevalent threats we've observed between March 24 and March 31. As with previous roundups, this post isn't meant to be an in-depth analysis."

Threat Source newsletter (March 30, 2023) — It's impossible to tell if your home security camera or doorbell is truly safe

Source: https://blog.talosintelligence.com/threat-source-newsletter-march-30-2023/

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.

From the Article: "Everyone loves a good video of someone slipping on their icy steps in the winter, captured thanks to their home security camera or smart doorbell. But what about when that camera is just kind of chilling out and not catching the moment your dog takes off after that squirrel?"

Spyware vendors use exploit chains to take advantage of patch delays in mobile ecosystem

Source: https://www.csoonline.com/article/3692354/spyware-vendors-use-exploit-chains-to-take-advantage-of-patch-delays-in-mobile-ecosystem.html

From the Article: "Several commercial spyware vendors developed and used zero-day exploits against iOS and Android users last year. However, their exploit chains also relied on known vulnerabilities to work, highlighting the importance of both users and device manufacturers to speed up the adoption of security patches."

5 cyber threats retailers are facing — and how they're fighting back

Source: https://www.csoonline.com/article/3691821/5-cyber-threats-retailers-are-facing-and-how-they-re-fighting-back.html

From the Article: "There are many reasons retailers are juicy targets for hackers. They earn and handle tremendous amounts of money, store millions of customer credit card numbers, and have frontline staff who may lack cybersecurity training. To save money, some retailers use older equipment that isn't adequately updated, secured, or monitored to deal with cyberattacks. "

LockBit leaks data stolen from the South Korean National Tax Service

Source: https://securityaffairs.com/144342/cyber-crime/lockbit-south-korean-national-tax-service.html

From the Article: "On March 29, 2023, The Lock Bit ransomware gang announced the hack of the South Korean National Tax Service. The group added the South Korean agency to its Tor leak site and announced the release of stolen data by April 1st, 2023 in case the ransom was not paid."

Link back to Table of Contents

New AlienFox toolkit harvests credentials for tens of cloud services

Source: https://securityaffairs.com/144239/cyber-crime/alienfox-toolset-cloud-service-providers.html

From the Article: "AlienFox is available for sale and is primarily distributed on Telegram in the form of source code archives. Some modules are available on GitHub allowing threat actors to customize their malicious code to suit their needs."

Emotet is back after a three-month hiatus

Source: https://securityaffairs.com/143722/cyber-crime/emotet-microsoft-onenote-campaign.html

From the Article: "The Emotet malware returns after a three-month hiatus and threat actors are distributing it via Microsoft OneNote email attachments to avoid detection."

Weekly Cyber Threat Report, March 27 – March 31, 2023

Source: https://cyberintelmag.com/threat-intelligence/weekly-cyber-threat-report-march-27-march-31-2023/

From the Article: "This week's good news includes US President Biden issuing an order to ban commercial spyware, a Nigerian BEC scammer being imprisoned in the US, account takeover flaws in ChatGPT being patched by OpenAI, Microsoft updating the Azure Cloud Service to fix a dangerous RCE vulnerability, and much more."

SafeMoon: Threat Actors Exploit the "Burn" Bug, Stealing $8.9M From Liquidity Pool

Source: https://www.cysecurity.news/2023/04/safemoon-threat-actors-exploit-burn-bug.html

From the Article: "The SafeMoon token liquidity pool lost $8.9 million, after a threat actor took advantage of a recently developed "burn" smart contract function that artificially inflate the token price, enabling the actors to sell SafeMoon at a much higher price. "

Ransomware Threats in 2023: Increasing and Evolving

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

Source: https://www.cysecurity.news/2023/04/ransomware-threats-in-2023-increasing.html

From the Article: "Cybersecurity threats are increasing every year, and 2023 is no exception. In February 2023, there was a surge in ransomware attacks, with NCC Group reporting a 67% increase in such attacks compared to January. The attacks targeted businesses of all sizes and industries, emphasizing the need for organizations to invest in robust cybersecurity measures."

The Risks of Automatic Updates: A Closer Look at the Malicious 3CX Update

Source: https://www.cysecurity.news/2023/04/the-risks-of-automatic-updates-closer.html

From the Article: "The attackers had managed to gain access to 3CX's update servers and replace a legitimate software update with a malicious version. This update, which was automatically installed on thousands of 3CX systems, contained a backdoor that gave the attackers full access to the compromised systems. "

Protect Yourself from Healthcare Cyber Risks

Source: https://www.cysecurity.news/2023/04/protect-yourself-from-healthcare-cyber.html

From the Article: "It has become increasingly apparent in the past few years that technology has played a significant role to assist hospitals and patients in managing their interactions. "

This New AlienFox Toolkit Steals Credentials for 18 Cloud Services

Source: https://www.cysecurity.news/2023/03/this-new-alienfox-toolkit-steals.html

From the Article: "Threat actors can use a new modular toolkit called 'AlienFox' to scan for misconfigured servers and steal authentication secrets and credentials for cloud-based email services."

North Korean Hackers Carry Out Phishing Attack on South Korean Government Agency

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

Source: https://www.cysecurity.news/2023/03/north-korean-hackers-carry-out-phishing.html

From the Article: "North Korean hackers recently executed a phishing attack on a South Korean government agency using social engineering tactics, as reported on March 28th, 2023."

DataDome Closes $42M in Series C Funding to Advance the Fight Against Bot-Driven Cyberattacks and Fraud

Source: https://www.darkreading.com/attacks-breaches/datadome-closes-42m-in-series-c-funding-to-advance-the-fight-against-bot-driven-cyberattacks-and-fraud

From the Article: "The investment will fund global commercial rollout and R&D efforts to debilitate fraudsters."

WordPress WooCommerce 7.1.0 Remote Code Execution

Source: https://packetstormsecurity.com/files/171609/wpwoocommerce710-exec.txt

From the Article: "WordPress WooCommerce plugin version 7.1.0 suffers from a remote code execution vulnerability."

Application specialist and vulnerability management leaders forge partnership for secure patching process

Source: https://www.flexera.com/blog/vulnerability-management/vulnerability-management-leaders-forge-partnership-for-secure-patching/

From the Article: "There’s no getting around it: Today’s digital world requires businesses to rely heavily on software to run their operations, manage data and communicate with customers. But this widespread use of software also presents a significant risk to cybersecurity."

ChatGPT Ready to Write Ransomware But Failed to Go Deep

Source: https://gbhackers.com/chatgpt-ready-to-write-ransomware/

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

From the Article: "Our lives are now enriched by the availability of LLMs that are easily accessible on the internet, so we have tools such as the ChatGPT that can help us breathe life into even the most abstract ideas."

Winnti APT Hackers Attack Linux Servers With New Malware 'Mélofée'

Source: https://gbhackers.com/winnti-linux-servers/

From the Article: "The discovery of a novel malware piece targeting Linux servers has been attributed to an unknown Chinese state-sponsored hacking group. ExaTrack, a French security firm, recently reported that the malware in question was named Mélofée."

Chinese Hackers Using KEYPLUG Backdoor to Attack Windows & Linux Systems

Source: https://gbhackers.com/chinese-hackersckeyplug-backdoor/

From the Article: "It has been reported by the Recorded Future's Insikt Group that RedGolf, a Chinese state-sponsored threat actor group, was using a backdoor designed especially for Windows and Linux systems called KEYPLUG to infiltrate networks."

Hack the Pentagon website promotes the benefits of bug bounties to US Military

Source: https://www.bitdefender.com/blog/hotforsecurity/hack-the-pentagon-website-promotes-the-benefits-of-bug-bounties-to-us-military/

From the Article: "My guess is that if you stumbled across a website that called itself "Hack the Pentagon" and was decorated with a grisly-looking skull, you would probably think that you might be somewhere less than legitimate."

Ukrainian Hacktivists Trick Russian Military Wives for Personal Info

Source: https://www.hackread.com/ukrainian-hacktivists-russian-military-wives/

From the Article: "Ukrainian hacktivists extracted personal information, including sensitive military data and even nude photos of one of the targeted military wives."

Link back to Table of Contents

Zimbra email platform vulnerability exploited to steal European govt emails

Source: https://www.hackread.com/zimbra-email-platform-vulnerability-phishing-scam/

From the Article: "Researchers have noted that attackers are targeting a medium-severity Zimbra vulnerability that the company patched in version 9.0.0 Patch 24, one year ago."

IRS tax forms W-9 email scam drops Emotet malware

Source: https://www.hackread.com/irs-tax-forms-w-9-email-scam-emotet-malware/

From the Article: "Researchers have warned users to be on alert, as the IRS never sends emails to confirm taxpayers' personal information."

Vulnerability Enabled Bing.com Takeover, Search Result Manipulation

Source: https://www.hackread.com/bing-search-result-takeover-vulnerability/

From the Article: "Cybersecurity researchers at Wiz reported the vulnerability to Microsoft and dubbed the attack "BingBang"."

The 10 Best Cybersecurity Companies in the UK

Source: https://www.hackread.com/the-10-best-cybersecurity-companies-in-the-uk/

From the Article: "When it comes to cybersecurity companies in the United Kingdom, there are lots to choose from, However, since their services aren't all the same or at the same level, you'll only want to work with the best ones."

Sundry Files - 274,461 breached accounts

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

From the Article: "In January 2022, the now defunct file upload service Sundry Files

Link back to Table of Contents

suffered a data breach that exposed 274k unique email addresses. The data also included usernames, IP addresses and passwords stored as salted SHA-256 hashes."

Evolving AlienFox Malware Steals Cloud Services Credentials

Source: https://www.bankinfosecurity.com/evolving-alienfox-malware-steals-cloud-services-credentials-a-21594

From the Article: "Hackers have used a modular toolkit called "AlienFox"' to compromise email and web hosting services at 18 companies. Distributed mainly by Telegram, the toolkit scripts are readily available in open sources such as GitHub, leading to constant adaptation and variation in the wild."

Subprime Lender TitleMax Hit With Hacking Incident

Source: https://www.bankinfosecurity.com/subprime-lender-titlemax-hit-hacking-incident-a-21592

From the Article: "The parent company of subprime lender TitleMax says hackers made off the Social Security numbers and financial account information of up to nearly 5 million individuals."

3 More Healthcare Entities Report Website Tracking Breaches

Source: https://www.bankinfosecurity.com/3-more-healthcare-entities-report-website-tracking-breaches-a-21590

From the Article: "Three more healthcare organizations have joined the growing list of entities reporting large data breaches to federal regulators involving the previous use of tracking codes on their websites."

Spyware Campaigns Exploited Zero-Day iOS and Android Flaws

Source: https://www.bankinfosecurity.com/spyware-campaigns-exploited-zero-day-ios-android-flaws-a-21578

From the Article: "Google says it spotted two "highly targeted" advanced spyware

Link back to Table of Contents

campaigns using zero-days in the Android and iOS operating systems and vulnerabilities in the Samsung Internet Browser. "

Cryptohack Roundup: Euler Finance, SafeMoon, BitKeep

Source: https://www.bankinfosecurity.com/cryptohack-roundup-euler-finance-safemoon-bitkeep-a-21576

From the Article: "Every week, Information Security Media Group rounds up cybersecurity incidents in the world of digital assets. In focus between March 24 and 30: SafeMoon, an update on Euler Finance, crypto-stealing Clipper malware, BitKeep, theft fail at Swerve Finance, THORChain, APT43 and an update on ParaSpace."

Leaks Reveal Moscow Source for Hacking, Disinformation Tools

Source: https://www.bankinfosecurity.com/leaks-reveal-moscow-source-for-hacking-disinformation-tools-a-21571

From the Article: "Leaked documents from a Moscow IT consultancy reveal how the Russian government has commissioned tools for its military and intelligence agencies for conducting cyber operations, information warfare, and controlling the internet, as well as training critical infrastructure hackers."

Smart Grid Fragility, a Constant Threat for the European and American Way of Living

Source: https://heimdalsecurity.com/blog/smart-grid-fragility-a-constant-threat-for-the-european-and-american-way-of-living/

From the Article: "In today's world, a multitude of smart devices helps us to improve our lives, as we rely more and more on technology for a comfortable and efficient lifestyle – smart appliances, smart cars, smartwatches. "

37M Subscribers Streaming Platform Lionsgate Exposes User Data

Source: https://heimdalsecurity.com/blog/37m-subscribers-streaming-platform-lionsgate-exposes-user-data/

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

From the Article: "Cybersecurity researchers found that Lionsgate, an entertainment industry giant, exposed the IP addresses and viewing habits of its subscribers. The investigators from Cybernews uncovered that the video-streaming service Lionsgate Play had exposed user information via a publicly accessible ElasticSearch instance."

Week in review: 3CX supply chain attack, ChatGPT data leak

Source: https://www.helpnetsecurity.com/2023/04/02/week-in-review-3cx-supply-chain-attack-chatgpt-data-leak/

From the Article: "Here's an overview of some of last week's most interesting news, articles, interviews and videos: Visa fraud expert outlines the many faces of payment ecosystem fraud In this Help Net Security interview, Michael Jabbara, the VP and Global Head of Fraud Services at Visa, delves into digital skimming attacks, highlighting their common causes, and provides insights into what measures merchants can take to prevent them."

Overcoming obstacles to introduce zero-trust security in established systems

Source: https://www.helpnetsecurity.com/2023/03/31/michal-cizek-goodaccess-introduce-zero-trust-security/

From the Article: "In this Help Net Security interview, Michal Cizek, CEO at GoodAccess, discusses the crucial balance between leveraging distributed resources and maintaining top-notch security measures. "

OSC&R open software supply chain attack framework now on GitHub

Source: https://www.helpnetsecurity.com/2023/03/31/oscar-open-software-supply-chain-attack-framework-github/

From the Article: "OSC&R (Open Software Supply Chain Attack Reference) is an open framework for understanding and evaluating software supply chain security threats. It has received the endorsement of former U.S. NSA Director Admiral Mike Rogers, and is now available on GitHub. "

ReasonLabs Dark Web Monitoring identifies malicious online activity

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

Source: https://www.helpnetsecurity.com/2023/03/31/reasonlabs-dark-web-monitoring/

From the Article: "ReasonLabs has launched a Dark Web Monitoring feature to its RAV Online Security solution, a web extension that provides real-time, 24/7 protection against a range of malicious online activity."

Cynerio and Sodexo join forces to address growing threats to medical IoT devices

Source: https://www.helpnetsecurity.com/2023/03/31/cynerio-sodexo/

From the Article: "Cynerio has formed a partnership with Sodexo to provide hospitals and healthcare systems with visibility into their IoMT footprint that allows for the immediate remediation of identified threats through step-by-step mitigation recommendations for each attack and risk."

Scan and diagnose your SME's cybersecurity with expert recommendations from ENISA

Source: https://www.helpnetsecurity.com/2023/03/30/enisa-scan-diagnose-sme-cybersecurity/

From the Article: "The release of a cybersecurity maturity assessment tool by the European Union Agency for Cybersecurity (ENISA) aims to provide Small and Medium Enterprises (SMEs) with a valuable resource for enhancing their security posture. "

Anomali and Canon IT join forces to combat zero-day threats

Source: https://www.helpnetsecurity.com/2023/03/30/anomali-canon-it/

From the Article: "Anomali and Canon IT Solutions have announced the availability of the Canon IT Solutions "Threat Intelligence Platform," a security operations service that operationalizes threat intelligence to better detect and respond to attacks."

Space ISAC sets up Operational Watch Center to monitor spread of threats, vulnerabilities to space systems

Source: https://industrialcyber.co/analysis/space-isac-sets-up-operational-watch-center-to-monitor-spread-of-threats-vulnerabilities-to-space-systems/

Link back to Table of Contents

From the Article: "Space ISAC launched Thursday its Operational Watch Center and its initial operational capability. Supported by a dedicated team of ten in-person analysts with additional virtual support enabled by a secure cloud architecture, Space ISAC's Watch Center represents a monumental step forward for the space community. "

CyManII, Tooling U-SME offer cybersecurity training to develop critical workforce skills across manufacturing sector

Source: https://industrialcyber.co/training/cymanii-tooling-u-sme-offer-cybersecurity-training-to-develop-critical-workforce-skills-across-manufacturing-sector/

From the Article: "The Cybersecurity Manufacturing Innovation Institute (CyManII) partnered with Tooling U-SME, a workforce training and development arm of SME, to launch a cybersecurity training program called CyManII Sealed."

FERC approves Reliability Standard CIP-003-9 covering supply chain risk management of low-impact BES cyber systems

Source: https://industrialcyber.co/nerc-cip/ferc-approves-reliability-standard-cip-003-9-covering-supply-chain-risk-management-of-low-impact-bes-cyber-systems/

From the Article: "The U.S. Federal Energy Regulatory Commission (FERC) published an order approving the proposed Reliability Standard CIP-003-9 put forward by the North American Electric Reliability Corporation (NERC) in December. The agency also approved the associated implementation plan, associated violation risk factors, violation severity levels, and the retirement of the currently effective Commission-approved Reliability Standard CIP-003-8 immediately prior to the effective date of Reliability Standard CIP-003-9."

Maintaining Data Integrity With Growing Cybersecurity Concerns

Source: https://informationsecuritybuzz.com/data-integrity-cybersecurity-concerns/

From the Article: "The significance of keeping data integrity has never been more important in a world where data breaches appear to occur every day. It is because cybersecurity threats are expanding at an alarming rate."

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.

Thieves Steal $9m from Crypto Liquidity Pool

Source: https://www.infosecurity-magazine.com/news/thieves-steal-9m-crypto-liquidity/

From the Article: "SafeMoon claims exploited vulnerability was to blame."

Modular "AlienFox" Toolkit Used to Steal Cloud Service Credentials

Source: https://www.infosecurity-magazine.com/news/alienfox-toolkit-steal-cloud/

From the Article: "Harvesting API keys and secrets from AWS SES, Microsoft Office 365 and other services."

Ukrainian Police Bust Multimillion-Dollar Phishing Gang

Source: https://www.infosecurity-magazine.com/news/ukrainian-police-bust-phishing/

From the Article: "More than 100 sites created to lure European victims."

For Cybersecurity, the Tricks Come More Than Once a Year

Source: https://www.itsecurityguru.org/2023/03/31/for-cybersecurity-the-tricks-come-more-than-once-a-year/

From the Article: "Anyone who pays attention on April Fool's Day has learned to think twice about the information they read, the links they receive and the people who try impersonating others. The irony, though, is that while we're hypervigilant against these harmless pranks, malicious actors are trying to play the same types of tricks on us day in and day out. "

Only 10% of workers remember all their cyber security training

Source: https://www.itsecurityguru.org/2023/03/30/only-10-of-workers-remember-all-their-cyber-security-training/

From the Article: "New research by CybSafe found only 10% of workers remember all their cybersecurity 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.

JTEKT ELECTRONIC Screen Creator Advance 2 vulnerable to improper restriction of operations within the bounds of a memory buffer

Source: https://jvn.jp/en/vu/JVNVU99710864/

From the Article: "Screen Creator Advance 2 provided by JTEKT ELECTRONICS CORPORATION is vulnerable to improper restriction of operations within the bounds of a memory buffer."

HAProxy vulnerable to HTTP request/response smuggling

Source: https://jvn.jp/en/jp/JVN38170084/

From the Article: "HAProxy contains a HTTP request/response smuggling vulnerability."

German Police Raid DDoS-Friendly Host 'FlyHosting'

Source: https://krebsonsecurity.com/2023/03/german-police-raid-ddos-friendly-host-flyhosting/

From the Article: "Authorities in Germany this week seized Internet servers that powered FlyHosting, a dark web offering that catered to cybercriminals operating DDoS-for-hire services, KrebsOnSecurity has learned."

Study Reveals WiFi Protocol Vulnerability Exposing Network Traffic

Source: https://latesthackingnews.com/2023/03/31/study-reveals-wifi-protocol-vulnerability-exposing-network-traffic/

From the Article: "According to a recent study, the existing WiFi protocol IEEE 802.11 has an innate security vulnerability in its design that risks users' privacy. The researchers from Northeastern University and imec-DistriNet, KU Leuven, have shared their findings in a detailed research paper."

Link back to Table of Contents

Hacking Campaign Exploited Zero Day Tied To Spyware Firm

Source: https://www.scmagazine.com/news/device-security/hack-campaign-zero-day-spyware-firm

From the Article: "A spyware campaign driven by "mercenary" hackers exploited a zero-day vulnerability in Android devices, reported Amnesty International's Security Labs."

3 tips for creating backups your organization can rely on when ransomware strikes

Source: https://www.malwarebytes.com/blog/news/2023/03/3-tips-for-creating-backups-your-organization-can-rely-on-when-ransomware-strikes

From the Article: "Backups are an organization's last line of defense against ransomware, because comprehensive, offline, offsite backups give you a chance to restore or rebuild your computers without paying a criminal for a decryption key."

The Rising Trend of OneNote Documents for Malware delivery

Source: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/rising-trend-of-onenote-documents-for-malware-delivery/

From the Article: "McAfee Labs has recently observed a new Malware campaign which used malicious OneNote documents to entice users to click on an embedded file to download and execute the Qakbot trojan."

AlienFox Toolset Harvests Credentials From 18 Cloud Services

Source: https://www.scmagazine.com/news/identity-and-access/alienfox-source-code-toolset-harvests-credentials-18-cloud-services

From the Article: "A comprehensive toolset dubbed "AlienFox" has been discovered harvesting credentials for up to 18 cloud service providers."

Is ChatGPT A Silver Bullet For Cybercriminals?

Source: https://www.forbes.com/sites/forbestechcouncil/2023/03/27/is-chatgpt-a-silver-

Link back to Table of Contents

bullet-for-cybercriminals/

From the Article: "By now, you've heard of ChatGPT—or more likely, you've heard that it's coming to take your job whether you're a programmer, journalist, musician or almost anything else."

Risk-based Vulnerability Management Combined With A Cyber Risk Management Platform

Source: https://blog.qualys.com/vulnerabilities-threat-research/2023/03/30/risk-based-vulnerability-management-combined-with-a-cyber-risk-management-platform

From the Article: "Recent insights from IDC's recent report, Worldwide Device Vulnerability Management Forecast, 2023–2027: Evolving Beyond Scanning (Feb. 2023), provide a sobering look at the future of what cybersecurity stacks may look like in a few years. "

4 Reasons Why Application Security is a Dedicated Discipline Within Cybersecurity

Source: https://blog.radware.com/application-security-4/2023/03/4-reasons-why-application-security-is-a-dedicated-discipline-within-cybersecurity/

From the Article: "As web applications become the core of business functions, application protection takes an ever more important role in protecting those applications, their availability and the customer data that is processed through them."

How Ukraine's Premier Electronics Retailer Ended Bot Attacks on its Digital Storefront

Source: https://blog.radware.com/uncategorized/2023/03/how-ukraines-premier-electronics-retailer-ended-bot-attacks/

From the Article: "With the accelerated growth of online retailers — especially after the Covid pandemic — we are witnessing an alarming rise in the deployment of malicious bots. While it's certainly the case during the holiday sales season, digital storefronts are open year around."

US cyber spymaster calls TikTok China's 'Trojan horse' - The Register

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/2023/03/29/china_tiktok_trojan_horse/

From the Article: "Joyce, speaking at the Silverado Policy Accelerator's conference on Monday, called TikTok "a strategic issue." This, as opposed to the type of tactical, day-to-day cyber threats the US spy agency wards off on the regular from nation-state actors and cyber crime gangs looking to make a buck (coin?) from business email compromise or ransomware infections."

Next-gen solution for ransomware data recovery - Cubbit

Source: https://www.cubbit.io/solution-for-ransomware-data-recovery

From the Article: "Protect your business data from ransomware and accidental deletion while maintaining compliance with audit and retention requirements. Just choose what data you want to make immutable, along with an expiration date: within this period, no one — nor hackers, nor ransomware, nor Cubbit — can delete, encrypt, or modify your data."

Dish Faces Investor Lawsuit Over Ransomware Attack, Downgrades From Equity Analysts

Source: https://www.nexttv.com/news/99-problems-dish-faces-investor-lawsuits-over-ransomware-attack-downgrades-from-equity-analysts

From the Article: "The satellite-TV provider turned nascent 5G wireless company is still recovering from a ransomware attack (opens in new tab) that has shut down or otherwise hampered the performance of critical internal networks for the better part of the month, while compromising private customer data. "

Lewis & Clark College cyberattack claimed by notorious ransomware gang

Source: https://therecord.media/lewis-clark-college-ransomware-attack-vice-society

From the Article: "The Vice Society cybercrime group took credit for the attack on Friday, posting samples of passports as well as documents that included Social Security numbers, insurance files, W-9 forms, contracts and more."

Link back to Table of Contents

TASB Risk Management Fund Aids Cybersecurity Efforts

Source: https://www.tasb.org/members/Enhance-District/School-District-Cybersecurity/

From the Article: "Cybersecurity is a topic of keen interest for school district officials these days. Lines for cybersecurity sessions snaked down the hallways at the recent Texas Computer Education Association conference in San Antonio. In one room, about 50 educators and administrators crowded around a tabletop exercise discussing phishing, ransomware, and other cyber issues. "

Ransomware attacks skyrocket as threat actors double down on U.S., global attacks

Source: https://www.techrepublic.com/article/nccgroup-ransomware-attacks-up-february/

From the Article: "New studies by NCC Group and Barracuda Networks show threat actors are increasing ransomware exploits, with consumer goods and services receiving the brunt of attacks and a large percentage of victims being hit multiple times."

Ransomware Actors Target IBM's Aspera Faspex - Gridinsoft Blogs

Source: https://gridinsoft.com/blogs/ransomware-actors-target-aspera-faspex/

From the Article: "File transfer utility Aspera Faspex, developed by IBM, became a riding mare of cybercriminals. A vulnerability discovered in the past year is exploited to deploy various ransomware samples. Key threat actors using that breach are IceFire, Shadowserver and Buhti. The issue allows arbitrary code execution, and touches all app versions before Faspex 4.4.2 PL2."

13 Expert Tips To Defend Against And Respond To Ransomware Attacks - Forbes

Source: https://www.forbes.com/sites/forbestechcouncil/2023/03/31/13-expert-tips-to-defend-against-and-respond-to-ransomware-attacks/

From the Article: "In February 2023, the city of Oakland was forced to take multiple systems offline for several days after being hit with a successful ransomware attack; the hackers also released the personal data of city employees online a few weeks later."

Link back to Table of Contents

Ransomware attacks: is your supply chain software safe? - Raconteur

Source: https://www.raconteur.net/supply-chain/ransomware-attacks-is-your-supply-chain-software-safe/

From the Article: "In a world where cybercriminals run amok, it's no longer a case of if your business will be hit with an attack, but when. And supply chain teams are particularly vulnerable. Gartner predicts that by 2025, 45% of organisations worldwide will have experienced an attack against their supply chain software – a threefold jump from 2021."

Maryland Hospital Reveals 30K Individuals Impacted by Ransomware Attack

Source: https://healthitsecurity.com/news/maryland-hospital-reveals-30k-individuals-impacted-by-ransomware-attack

From the Article: "Atlantic General Hospital has notified 30,704 patients of a ransomware attack that potentially compromised protected health information (PHI), a notice provided to the Maine Attorney General's Office stated. "

ConnectWise Releases 2023 MSP Threat Report with Insights into Top Ransomware ...

Source: https://finance.yahoo.com/news/connectwise-releases-2023-msp-threat-132200549.html

From the Article: "TAMPA, Fla., March 31, 2023 (GLOBE NEWSWIRE) -- ConnectWise, the world's leading software company dedicated to the success of IT solution providers (TSPs), today announced the findings of its annual MSP Threat Report."

Recovering from a Ransomware Attack on Your RAID System - Geeky Gadgets

Source: https://www.geeky-gadgets.com/recovering-from-a-ransomware-attack-on-your-raid-system-31-03-2023/

From the Article: "Did you know in the first half of 2022, there were 236.1 million ransomware attacks worldwide? The attacks are increasing everywhere as hackers adopt highly deceiving methods to attack systems."

Link back to Table of Contents

1/3 organisations hit with ransomware are repeat victims - IT Brief Australia

Source: https://itbrief.com.au/story/1-3-organisations-hit-with-ransomware-are-repeat-victims

From the Article: "Barracuda Networks has published its 2023 Ransomware Insights report, which shows that 69% of the organisations surveyed in Australia were hit with at least one successful ransomware attack in 2022 and 33% say they were hit twice or more. "

New Cylance Ransomware strain emerges, experts speculate about its notorious members

Source: https://www.itpro.co.uk/security/ransomware/370362/new-cylance-ransomware-strain-experts-speculate-notorious-members

From the Article: "A new ransomware strain with the name 'Cylance Ransomware' has been unearthed by security researchers, in what could be a new lease of life for long-time threat actors."

4 steps to avoid a ransomware attack - eSchool News

Source: https://www.eschoolnews.com/it-leadership/2023/03/30/4-steps-to-avoid-a-ransomware-attack/

From the Article: "Educational institutions have an urgent reason to put data security and backup at the top of their agenda: the rising threat of ransomware. Security firm BlackFog reports that the education sector is now the top target for ransomware attacks, surpassing government and healthcare."

Ransomware attacks rise 45% in Feb, LockBit ramps up activity - SecurityBrief New Zealand

Source: https://securitybrief.co.nz/story/ransomware-attacks-rise-45-in-feb-lockbit-ramps-up-activity

From the Article: "Analysis from NCC Group's Global Threat Intelligence team has revealed there were 240 ransomware attacks in February, a 45% increase from January. "

Link back to Table of Contents

FBI Agent Discusses Trends in Ransomware at Municipal Law Symposium - Erie News Now

Source: https://www.erienewsnow.com/category/270070/high-school-sports

From the Article: "A supervisory special agent from the Pittsburgh FBI office was the keynote speaker. Part of his focus: a talk about trends in ransomware."

A hospital went dark after it was hacked. It's still reeling two years later - WFYI

Source: https://www.wfyi.org/news/articles/a-hospital-went-dark-after-it-was-hacked-its-still-reeling-two-years-later

From the Article: "Matt Ashley, a senior IT technologist at Johnson Memorial Health in Franklin, Indiana, is part of a small team that has been working for months after the cyberattack. His office is lined with dead computer screens and CPUs that his team has had to thoroughly inspect to make sure there is no malware the hackers might have left behind."

Indian pharmaceutical giant warns of revenue loss, litigation after ransomware attack

Source: https://therecord.media/sun-pharma-india-ransomware-attack

From the Article: "The largest pharmaceutical company in India confirmed a ransomware attack in its regulatory filings this week, explaining that the incident involved the theft of company data and personal information."

Clop ransomware group triggers new attack spree, hitting household brands

Source: https://www.cybersecuritydive.com/news/ransomware-spree-goanywhere/646152/

From the Article: "A ransomware threat actor is exploiting a vulnerability in GoAnywhere to launch a spree of attacks, claiming dozens of additional victims, according to threat researchers."

Link back to Table of Contents

A Hacker's Mind News

Source: https://www.schneier.com/blog/archives/2023/03/a-hackers-mind-news-2.html

From the Article: "My latest book continues to sell well. Its ranking hovers between 1,500 and 2,000 on Amazon. It's been spied in airports."

Hackers are actively exploiting a flaw in the Elementor Pro WordPress plugin

Source: https://securityaffairs.com/144290/hacking/elementor-pro-wordpress-plugin-critical-bug.html

From the Article: "WordPress security firm PatchStack warns of a high-severity vulnerability in the Elementor Pro WordPress plugin that is currently being exploited by threat actors in the wild."

Super FabriXss vulnerability in Microsoft Azure SFX could lead to RCE

Source: https://securityaffairs.com/144251/hacking/azure-service-fabric-explorer-super-fabrixss.html

From the Article: "Researchers shared details about a flaw, dubbed Super FabriXss, in Azure Service Fabric Explorer (SFX) that could lead to unauthenticated remote code execution."

Report: Chinese State-Sponsored Hacking Group Highly Active

Source: https://www.securityweek.com/report-chinese-state-sponsored-hacking-group-highly-active/

From the Article: "Chinese hacking group linked previously to attacks on U.S. state government computers is still "highly active"."

Mandiant Investigating 3CX Hack as Evidence Shows Attackers Had Access for Months

Source: https://www.securityweek.com/mandiant-investigating-3cx-hack-as-evidence-

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.

shows-attackers-had-access-for-months/

From the Article: "Several cybersecurity companies have published blog posts, advisories and tools to help organizations that may have been hit by the 3CX supply chain attack."

Severe Azure Vulnerability Led to Unauthenticated Remote Code Execution

Source: https://www.securityweek.com/severe-azure-vulnerability-led-to-unauthenticated-remote-code-execution/

From the Article: "A high-severity vulnerability in Azure Service Fabric Explorer could have allowed a remote, unauthenticated attacker to execute arbitrary code."

Cybersecurity Snapshot: CISA Issues Incident Response Tool for Microsoft Cloud Services

Source: https://www.tenable.com/blog/cybersecurity-snapshot-cisa-issues-incident-response-tool-for-microsoft-cloud-services

From the Article: "Learn about a free tool for detecting malicious activity in Microsoft cloud environments. Plus, Europol warns about ChatGPT cyber risks. Also, how business email compromise (BEC) scammers are stealing merchandise. In addition, CISA alerts orgs about early-stage ransomware breaches."

An open letter asks for a pause in advanced AI development. 3CXDesktopApp vulnerability and supply chain risk. The Vulkan papers.

Source: https://thecyberwire.com/newsletters/week-that-was/7/13

From the Article: "An open letter asks for a pause in advanced AI development. 3CXDesktopApp vulnerability and supply chain risk. The Vulkan papers. Threat actor movements observed and reported over the week."

Steve Benton, VP Anomali Threat Research & GM Belfast, shares a 'less is more' approach to cybersecurity.

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

Source: https://thecyberwire.com/podcasts/interview-selects/153/notes

From the Article: "This interview from March 31st, 2023 originally aired as a shortened version on the CyberWire Daily Podcast. In this extended interview, Dave Bittner sits down with Steve Benton, VP Anomali Threat Research & GM Belfast, to share a 'less is more' approach to cybersecurity."

Hackers Exploiting WordPress Elementor Pro Vulnerability: Millions of Sites at Risk!

Source: https://thehackernews.com/2023/04/hackers-exploiting-wordpress-elementor.html

From the Article: "Unknown threat actors are actively exploiting a recently patched security vulnerability in the Elementor Pro website builder plugin for WordPress."

Cacti, Realtek, and IBM Aspera Faspex Vulnerabilities Under Active Exploitation

Source: https://thehackernews.com/2023/04/cacti-realtek-and-ibm-aspera-faspex.html

From the Article: "Critical security flaws in Cacti, Realtek, and IBM Aspera Faspex are being exploited by various threat actors in hacks targeting unpatched systems."

Azure Serverless Security Risks Exposed by New Study

Source: https://www.trendmicro.com/en_us/research/23/c/azure-serverless-security-risks.html

From the Article: "Simulation uncovers hidden features and urges greater user awareness."

ICS/OT Cybersecurity 2022 TXOne Annual Report Insights

Source: https://www.trendmicro.com/en_us/research/23/c/ics-ot-cybersecurity-2022-txone-annual-report-insights.html

From the Article: "This article gives an in-depth overview of TXOne's insight report on ICS/OT cyber incidents."

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.

Pig butchering scams: The anatomy of a fast-growing threat

Source: https://www.welivesecurity.com/2023/03/29/pig-butchering-scams-anatomy-fast-growing-threat/

From the Article: "How fraudsters groom their marks and move in for the kill using tricks from the playbooks of romance and investment scammers."

Large-Scale AiTM Attack targeting enterprise users of Microsoft email services

Source: https://www.zscaler.com/blogs/security-research/large-scale-aitm-attack-targeting-enterprise-users-microsoft-email-services

From the Article: "ThreatLabz has discovered a new strain of a large-scale phishing campaign, which uses adversary-in-the-middle (AiTM) techniques along with several evasion tactics. Similar AiTM phishing techniques were used in another phishing campaign described by Microsoft recently here."

DBatLoader: Actively Distributing Malwares Targeting European Businesses

Source: https://www.zscaler.com/blogs/security-research/dbatloader-actively-distributing-malwares-targeting-european-businesses

From the Article: "This Zscaler ThreatLabz research article investigates the latest malware campaign of DBatLoader, which is being used by threat actors to target various businesses in European countries with Remcos RAT and Formbook."

The Unintentional Leak: A glimpse into the attack vectors of APT37

Source: https://www.zscaler.com/blogs/security-research/unintentional-leak-glimpse-attack-vectors-apt37

From the Article: "At Zscaler ThreatLabz, we have been closely monitoring the tools, techniques and procedures (TTPs) of APT37 (also known as ScarCruft or Temp.Reaper) - a North Korea-based advanced persistent threat actor. This threat actor has been very active in February and March 2023 targeting individuals in various South

Korean organizations."

Subscription Required

Chip equipment exports to China tumble as U.S. pushes decoupling

Source: https://asia.nikkei.com/Business/Tech/Semiconductors/Chip-equipment-exports-to-China-tumble-as-U.S.-pushes-decoupling

From the Article: "Impact could grow as Japan and Netherlands weigh their own restrictions"

Pentagon Woos Silicon Valley to Join Ranks of Arms Makers

Source: https://www.wsj.com/articles/pentagon-woos-silicon-valley-to-join-ranks-of-arms-makers-38b1d4c0?st

From the Article: "To keep up with China, the Defense Department is trying to lure private capital"

WSJ News Exclusive | Semiconductor Firms Asked to Submit Financial Projections to Get Chips Act Funds

Source: https://www.wsj.com/articles/semiconductor-firms-asked-to-submit-financial-projections-to-get-chips-act-funds-aafeba1a

From the Article: "Commerce Department will use financial statements to evaluate applications"

iOS 16.4—Apple Just Gave iPhone Users 33 Reasons To Update Now

Source: https://www.forbes.com/sites/kateoflahertyuk/2023/03/28/ios-164-apple-just-gave-iphone-users-33-reasons-to-update-now/

From the Article: "Apple's iOS 16.4 upgrade is finally here, along with a bunch of brilliant new iPhone features. There are also important security reasons to update to iOS 16.4, because the latest iPhone upgrade fixes 33 vulnerabilities, some of which are serious."

Link back to Table of Contents

Elon Musk, Other AI Experts Call for Pause in Technology's Development

Source: https://www.wsj.com/articles/elon-musk-other-ai-bigwigs-call-for-pause-in-technologys-development-56327f

From the Article: "Several tech executives and top artificial-intelligence researchers, including Tesla Inc. Chief Executive Officer Elon Musk and AI pioneer Yoshua Bengio, are calling for a pause in the breakneck development of powerful new AI tools."

WSJ News Exclusive | Semiconductor Firms Asked to Submit Financial Projections to Get Chips Act Funds

Source: https://www.wsj.com/articles/semiconductor-firms-asked-to-submit-financial-projections-to-get-chips-act-funds-aafeba1a?mod=Searchresults_pos2&page=1

From the Article: "Commerce Department will use financial statements to evaluate applications"

No 'Social Policy' in Chips Act Rules, Commerce Secretary Gina Raimondo Says

Source: https://www.wsj.com/articles/no-social-policy-in-chips-act-rules-commerce-secretary-gina-raimondo-says-616f156e?mod=Searchresults_pos5&page=1

From the Article: "Republicans say requiring grant applicants to provide child care and similar rules are aimed at advancing Biden administration's liberal agenda"

Micron Revives Some of Its Worst Memories

Source: https://www.wsj.com/articles/micron-revives-some-of-its-worst-memories-e3e6ff34?mod=Searchresults_pos7&page=1

From the Article: "Memory-chip maker is now losing billions as it writes down inventory to wait out downturn"

Link back to Table of Contents

U.S. 'Industrial Policy' Returns With $53 Billion for Chip Manufacturing

Source: https://www.wsj.com/video/series/wsj-explains/us-industrial-policy-returns-with-53-billion-for-chip-manufacturing/51099F5C-C981-4E8B-ADCA-0F740EF859FD?mod=Searchresults_pos8&page=1

From the Article: "Concerns about China's growth in chip manufacturing has helped create bipartisan consensus for boosting U.S. production"

Apparel Retailers Turn to Chips to Track Merchandise in Stores

Source: https://www.wsj.com/articles/apparel-retailers-expand-use-of-chips-to-track-merchandise-in-stores-21c37ce5?mod=Searchresults_pos9&page=1

From the Article: "Improving technology, lower costs and e-commerce demands are leading some merchants to beef up efforts to track individual items on the sales floor using RFID chips"

Japan Curbs Semiconductor-Gear Exports as Ties With China Chill

Source: https://www.wsj.com/articles/japan-restricts-semiconductor-equipment-exports-as-ties-with-china-chill-80885567?mod=Searchresults_pos11&page=1

From the Article: "Move comes as Tokyo's foreign minister plans to visit Beijing after detention of Japanese man"

Russia Supplies Iran With Cyber Weapons - Minute Briefing - WSJ Podcasts

Source: https://www.wsj.com/podcasts/minute-briefing/russia-supplies-iran-with-cyber-weapons/f93019d4-156f-40a4-bac1-00cbdacd63db?mod=Searchresults_pos12&page=1

From the Article: "Cyber military cooperation between Russia and Iran grows, worrying U.S. officials. Plus, Uber Eats to remove thousands of virtual brands from the app and semiconductor companies must prepare financial statements to apply for Chips Act funds. Julie Chang hosts."

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.

Toshiba Shareholders Draw the Short Stick, Again

Source: https://www.wsj.com/articles/toshiba-shareholders-draw-the-short-stick-again-fb3c57d3?mod=Searchresults_pos1&page=2

From the Article: "Toshiba's sale was supposed to be a bookend to years of corporate governance reforms in Japan"

FTC Chair Lina Khan Vows to Protect Competition in AI Market

Source: https://www.wsj.com/articles/ftc-chair-lina-khan-vows-to-protect-competition-in-ai-market-bb80e460?mod=Searchresults_pos6&page=2

From the Article: "Top antitrust official says big companies could panic and try to squelch competition"

Saudi Arabia Strengthens Relations With China Amid Strained U.S. Ties

Source: https://www.wsj.com/articles/saudi-arabia-strengthens-relations-with-china-amid-strained-u-s-ties-c5819114?mod=Searchresults_pos8&page=2

From the Article: "Riyadh is joining a Beijing-led political and security bloc; the two countries have also recently signed multibillion-dollar energy deals"

Dow Industrials Climb as Bank Concerns Ebb

Source: https://www.wsj.com/articles/global-stocks-markets-dow-update-03-27-2023-a066df06?mod=Searchresults_pos9&page=2

From the Article: "First Citizens shares jump after Silicon Valley Bank deal; Treasury yields rise"

Huawei's Meng Wanzhou Steps Closer to U.S.-China Tech-War Front Line as Chairwoman

Source: https://www.wsj.com/articles/huaweis-meng-wanzhou-steps-closer-to-u-s-china-tech-war-frontline-as-chairwoman-841fa779?mod=Searchresults_pos14&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: "Finance chief to rotate into post atop Chinese telecom company as U.S. considers tighter sanctions"

Microsoft, Google, Amazon Look to Generative AI to Lift Cloud Businesses

Source: https://www.wsj.com/articles/microsoft-google-amazon-look-to-generative-ai-to-lift-cloud-businesses-7159a43f?mod=Searchresults_pos15&page=2

From the Article: "Cloud providers are trying to use the tech behind ChatGPT to heat up demand"

China and Taiwan Relations Explained: What's Behind the Divide

Source: https://www.wsj.com/articles/china-taiwan-relations-tensions-explained-11653322751?mod=Searchresults_pos18&page=2

From the Article: "Beijing is flexing its military power in response to growing U.S. support for the island; here's a primer on the frictions"

Taiwan's President Lands in the U.S. Amid Threats From China

Source: https://www.wsj.com/articles/taiwans-president-lands-in-the-u-s-amid-threats-from-china-b7720379?mod=Searchresults_pos20&page=1

From the Article: "Beijing says Tsai Ing-wen's planned meeting with Speaker Kevin McCarthy could provoke retaliation"

WSJ News Exclusive | In Croatia, U.S. Campaigned to Stop Chinese Bid on Key Port

Source: https://www.wsj.com/articles/in-croatia-u-s-campaigned-to-stop-chinese-bid-on-key-port-58c9bbff?mod=Searchresults_pos1&page=2

From the Article: "Both the Trump and Biden administrations have worked with allies to limit Beijing's influence in Europe"

Link back to Table of Contents

Taiwan President's U.S. Trip Touches a Flashpoint in U.S.-China Ties

Source: https://www.wsj.com/articles/taiwan-presidents-u-s-trip-touches-a-flashpoint-in-u-s-china-ties-3a87c8b4?mod=Searchresults_pos2&page=2

From the Article: "Visit by Tsai Ing-wen is likely to determine whether relations between the U.S. and China deteriorate further"

Russia's Economy Is Starting to Come Undone

Source: https://www.wsj.com/articles/russias-economy-is-starting-to-come-undone-431a2878?mod=Searchresults_pos3&page=2

From the Article: "Investment is down, labor is scarce, budget is squeezed. Oligarch: 'There will be no money next year'"

In Walmart's Cyber Risk Formula, Every Bug Has a Backstory

Source: https://www.wsj.com/articles/in-walmarts-cyber-risk-formula-every-bug-has-a-backstory-b7762be1?mod=Searchresults_pos2&page=1

From the Article: "The retailer turned to actuaries, insurance experts, accountants and lawyers to help gauge security threats"

U.S. to Provide $25 Million to Costa Rica for Cybersecurity

Source: https://www.wsj.com/articles/u-s-to-provide-25-million-to-costa-rica-for-cybersecurity-b86be17c?mod=Searchresults_pos4&page=1

From the Article: "The aid will go to building a control center for cyber defenses in the country after a series of ransomware attacks last year"

Cybersecurity Workers Demand Higher Salaries

Source: https://www.wsj.com/articles/cybersecurity-workers-demand-higher-salaries-603d8218?mod=Searchresults_pos5&page=1

Link back to Table of Contents

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

From the Article: "Some corporate cyber chiefs are writing broader job ads and are allowing employees to work from different locations"

Biden Restricts Use of Commercial Hacking Tools by U.S. Agencies

Source: https://www.wsj.com/articles/biden-restricts-use-of-commercial-hacking-tools-by-u-s-agencies-f0a4afda?mod=Searchresults_pos6&page=1

From the Article: "Officials say at least 50 U.S. personnel overseas had been compromised by commercial spyware"

Pentagon Woos Silicon Valley to Join Ranks of Arms Makers

Source: https://www.wsj.com/articles/pentagon-woos-silicon-valley-to-join-ranks-of-arms-makers-38b1d4c0?mod=Searchresults_pos10&page=1

From the Article: "To keep up with China, the Defense Department is trying to lure private capital"

Pentagon Prepares for Space Warfare as Potential Threats From China, Russia Grow

Source: https://www.wsj.com/articles/pentagon-prepares-for-space-warfare-as-potential-threats-from-china-russia-grow-62a0623b?mod=Searchresults_pos11&page=1

From the Article: "White House's spending request includes plans for simulators, equipment to train Space Force members for battle"

Kamala Harris Pledges $100 Million to West Africa Nations to Fight Extremist Threat

Source: https://www.wsj.com/articles/kamala-harris-pledges-100-million-to-west-africa-nations-to-fight-extremist-threat-6f02504e?mod=Searchresults_pos3&page=2

From the Article: "Security aid will go to Ghana, Benin, Ivory Coast, Guinea and Togo after attacks in the region"

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.

Ukraine Calls for U.N. Security Council Meeting Over Belarus Nuclear Threat

Source: https://www.wsj.com/articles/ukraine-warns-against-russian-threat-to-put-nuclear-weapons-in-belarus-fd94ae39?mod=Searchresults_pos5&page=2

From the Article: "Western officials play down the significance of Russia stationing tactical nuclear weapons on Belarusian territory"

China Wants to Be at Center of New World Order, Top EU Official Says

Source: https://www.wsj.com/articles/china-wants-to-be-at-center-of-new-world-order-top-eu-official-says-22987030?mod=Searchresults_pos10&page=2

From the Article: "Trade bloc needs to defend its security and economic interests, she says ahead of trip to China"

WSJ News Exclusive | Microsoft Patched Bing Vulnerability That Allowed Snooping on Email and Other Data

Source: https://www.wsj.com/articles/microsoft-patched-bing-vulnerability-that-allowed-snooping-on-email-and-other-data-25b58831?mod=Searchresults_pos14&page=2

From the Article: "The issue was fixed days before the software company launched Bing with AI"

First Citizens Acquires Much of Failed Silicon Valley Bank - Minute Briefing - WSJ Podcasts

Source: https://www.wsj.com/podcasts/minute-briefing/first-citizens-acquires-much-of-failed-silicon-valley-bank/a0929c01-cd77-457e-bee7-d01a4cf710c5?mod=Searchresults_pos7&page=3

From the Article: "srael's largest labor union calls for a nationwide strike in response to Prime Minister Benjamin Netanyahu's plan to overhaul the judiciary. Ukraine seeks an emergency U.N. Security Council meeting over Russia's plan to put nuclear weapons in Belarus. Keith Collins hosts."

Link back to Table of Contents

Turkey's Parliament Ratifies Finland's NATO Membership Bid

Source: https://www.wsj.com/articles/turkeys-parliament-ratifies-finlands-nato-membership-bid-fb2b6aaa?mod=Searchresults_pos16&page=3

From the Article: "The move will allow for a historic expansion of the alliance"

Kevin McCarthy Pushes for Debt-Ceiling Talks as Unity Eludes GOP

Source: https://www.wsj.com/articles/kevin-mccarthy-pushes-for-debt-ceiling-talks-as-unity-eludes-gop-d6b2404d?mod=Searchresults_pos19&page=3

From the Article: "Joe Biden has demanded GOP produce budget as condition for negotiations on spending"

WSJ News Exclusive | China Is Sending Its Corruption Hunters to a Country Near You

Source: https://www.wsj.com/articles/china-deploys-its-corruption-hunters-abroad-a6484983?mod=Searchresults_pos18&page=5

From the Article: "G-20 nations among first destinations in move that risks intensifying alarm over expansion of Beijing's overseas activities"

North Korean Executions and Torture Alleged in New Report

Source: https://www.wsj.com/articles/north-korean-executions-and-torture-alleged-in-new-report-d5e94c98?mod=Searchresults_pos18&page=6

From the Article: "South Korea releases 450-page document as President Yoon Suk Yeol adds pressure on Pyongyang over rights abuses"

The Jobs Most Exposed to ChatGPT

Source: https://www.wsj.com/articles/the-jobs-most-exposed-to-chatgpt-e7ceebf0?mod=Searchresults_pos19&page=6

From the Article: "New study finds that AI tools could more quickly handle at least half of

the tasks that auditors, interpreters and writers do now"

U.S. Stops Sharing Data on Nuclear Forces With Russia

Source: https://www.wsj.com/articles/u-s-wont-share-data-on-nuclear-forces-with-russia-46700a50?mod=Searchresults_pos2&page=7

From the Article: "Biden administration seeks to encourage Moscow to return to compliance with New START treaty"

Technology Slump Refocuses Startups on Capital Discipline

Source: https://www.wsj.com/articles/technology-slump-refocuses-startups-on-capital-discipline-b5a8965a?mod=Searchresults_pos16&page=8

From the Article: "Falling investment valuations are resetting attitudes about cash flow and away from 'growth at all costs' in emerging markets"

Taiwan Leader's U.S. Visit Is Purposely Low-Key

Source: https://www.wsj.com/articles/taiwan-leaders-u-s-visit-is-purposely-low-key-f3f5b1ef?mod=Searchresults_pos12&page=8

From the Article: "Cautious atmosphere surrounds Tsai Ing-wen's stops in New York, while in China, her predecessor gets red-carpet welcome"

Higher Rates Are Coming for U.S. Companies

Source: https://www.wsj.com/articles/higher-rates-are-coming-for-u-s-companies-edbe2f23?mod=Searchresults_pos15&page=8

From the Article: "The interest-rate burden on most firms is still exceedingly low, but this will start to change over the next year"

Bank Turmoil Highlights Critical Role of Risk-Mitigation Technology

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.wsj.com/articles/bank-turmoil-highlights-critical-role-of-risk-mitigation-technology-96be4ab2?mod=Searchresults_pos13&page=9

From the Article: "In financial services, chief information officers are working more closely than ever with chief risk officers to ensure the right tools for analyzing risk are in place"

Too Much U.S. Government Information Is Classified, Report Finds

Source: https://www.wsj.com/articles/overclassification-problems-widespread-in-federal-government-report-finds-7fb98342?mod=Searchresults_pos4&page=10

From the Article: "White House, Congress seek solution to problem that has long bedeviled U.S. government"

U.S. Pushes for Business Investment in Africa to Counter China's Reach

Source: https://www.wsj.com/articles/u-s-pushes-for-business-investment-in-africa-to-counter-chinas-reach-9c48518b?mod=Searchresults_pos20&page=11

From the Article: "Vice President Kamala Harris is the latest American official to pledge more investment in the continent"

Artificial Intelligence Is Teaching Us New, Surprising Things About the Human Mind

Source: https://www.wsj.com/articles/artificial-intelligence-is-teaching-us-new-surprising-things-about-the-human-mind-ba7cdceb?mod=Searchresults_pos18&page=12

From the Article: "Thought is ever-changing electrical patterns unconnected to individual neurons. Meta is working on a system to read your mind."

Why Chinese Apps Are the Favorites of Young Americans

Source: https://www.wsj.com/articles/why-chinese-apps-are-the-favorites-of-young-americans-a9a5064a?mod=Searchresults_pos2&page=13

From the Article: "It isn't just the algorithms, but lessons from a competitive culture"

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 GOP Plan to Renew American Oil and Gas - Opinion: Potomac Watch - WSJ Podcasts

Source: https://www.wsj.com/podcasts/opinion-potomac-watch/the-gop-plan-to-renew-american-oil-and-gas/6e19608b-9161-4654-8a0f-0296e9be4982?mod=Searchresults_pos7&page=13

From the Article: "House Republicans make a push for H.R.1, the Lower Energy Costs Act, which Rep. Steve Scalise says will help make the U.S. less dependent on foreign oil. But can pieces of this legislation get through the Democratic Senate, and will Joe Manchin secure his permitting reform? Plus, Joe Biden changes course and approves the Willow drilling project in Alaska."

The Rise of Chinese Apps - The Journal. - WSJ Podcasts

Source: https://www.wsj.com/podcasts/the-journal/the-rise-of-chinese-apps/a148fe2f-f33f-4f61-bc4a-1485ef96c022?mod=Searchresults_pos12&page=13

From the Article: "While TikTok is getting a lot of scrutiny in Washington, other Chinese apps are on the rise. Four of the five hottest apps in the U.S. in March are tied to Chinese companies. But as WSJ's Shen Lu explains, some apps are now trying to distance themselves from their Chinese origins. "

The Paper-Thin Steel Needed to Power Electric Cars Is in Short Supply

Source: https://www.wsj.com/articles/the-paper-thin-steel-needed-to-power-electric-cars-is-in-short-supply-dbd2a78e?mod=Searchresults_pos17&page=1

From the Article: "U.S. Steel and Cleveland-Cliffs jockey with foreign rivals to supply the crucial material for EV motors"

New EV Rules Mean Fewer Models Eligible for Tax Credit

Source: https://www.wsj.com/articles/new-ev-rules-mean-fewer-models-eligible-for-tax-credit-98b6b63c?mod=Searchresults_pos18&page=1

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

From the Article: "Biden administration says it aims to reduce U.S. reliance on batteries and minerals from China"

New EV Tax-Credit Rules May Leave Some Cars in the Dust - Minute Briefing - WSJ Podcasts

Source: https://www.wsj.com/podcasts/minute-briefing/new-ev-tax-credit-rules-may-leave-some-cars-in-the-dust/64081093-36d9-49f8-ae02-a1d0e7252daa?mod=Searchresults_pos1&page=3

From the Article: "Plus: Inflation and consumer spending figures point to a possibly slowing economy. Italy's privacy regulator orders a temporary ban on OpenAI's ChatGPT. Pierre Bienaimé reports. "

U.S. Faces Electrician Shortage as It Tries to Go Green

Source: https://www.wsj.com/story/us-faces-electrician-shortage-as-it-tries-to-go-green-1b990742?mod=Searchresults_pos7&page=3

From the Article: "America is trying to install electic-car chargers, heat pumps and other gear deemed essential to address climate change, but the installers are in short supply"

China Opens Cybersecurity Probe of Micron Amid Competition With U.S. Over Technology

Source: https://www.wsj.com/articles/china-opens-cybersecurity-probe-of-micron-amid-competition-with-u-s-over-technology-57698d0a

From the Article: "Probe of U.S. chip maker follows rising tension between Beijing and Washington"

For Chip Makers, a Choice Between the U.S. and China Looms

Source: https://www.wsj.com/articles/for-chip-makers-a-choice-between-the-u-s-and-china-looms-5450df30?mod=Searchresults_pos1&page=1

From the Article: "Washington seeks to steer the semiconductor supply chain using

‘guardrails’ under the Chips Act"

They Posted Porn on Twitter. German Authorities Called the Cops

Source: https://www.wired.com/story/germany-twitter-porn-police/

From the Article: "Regulators are using an AI system to scan websites and messaging apps to find pornography. Creators face fines and potential prison sentences."

The US Is Sending Money to Countries Devastated by Cyberattacks - WIRED

Source: https://www.wired.com/story/white-house-costa-rica-albania-ransomware-aid/

From the Article: "Last spring, the Costa Rican government suffered a series of ransomware attacks that hobbled critical systems around the country. As imports and exports, healthcare, and other public services were disrupted, Costa Rican president Rodrigo Chaves Robles declared a state of emergency, and the recovery has been a months-long ordeal. "

$52 Billion Chipmaking Plan Is Racing Toward Failure

Source: https://www.bloomberg.com/opinion/articles/2023-03-28/chips-act-funding-isn-t-what-us-semiconductor-manufacturers-need#xj4y7vzkg

From the Article: “A big semiconductor bill was once a bipartisan showpiece. Ill-considered policies are killing it.”

Secret Trove Offers Rare Look Into Russian Cyberwar Ambitions

Source: https://www.washingtonpost.com/national-security/2023/03/30/russian-cyberwarfare-documents-vulkan-files/

From the Article: "The documents detail a suite of computer programs and databases that would allow Russia’s intelligence agencies and hacking groups to better find vulnerabilities, coordinate attacks and control online activity."

Link back to Table of Contents

He came to D.C. as a Brazilian student. The U.S. says he was a Russian spy.

Source: https://www.washingtonpost.com/world/2023/03/29/russian-spy-brazilian-student-washington/

From the Article: "Johns Hopkins graduate Victor Ferreira was unmasked as GRU operative Sergey Cherkasov, according to a federal indictment and Western security officials"

Link back to Table of Contents