Weekly Security Articles 28-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.

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

Live Webinar | Making the Connection Between Cybersecurity and Patient Care

Source: https://www.bankinfosecurity.com/webinars/live-webinar-making-connection-between-cybersecurity-patient-care-w-4778

May 2, 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

Digital Twin & Smart Manufacturing Summit
Source: https://digitaltwintechsummit.com/

April 27 - 28, 2023

CISO Leaders Summit Australia 2022

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

May 2, 2023

ThotCon - Chicago's Hacking Conference

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-

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

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

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

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

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

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

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

DEF CON 31

Source: https://defcon.org/

August 10-13, 2023

2023 PCI North America Community Meeting

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

September 12-14, 2023

Mind The Sec

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

September 12-14, 2023

Critical Infrastructure Protection & Resilience Europe

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

September 26-28, 2023

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

Source: https://www.gartner.com/en/conferences/emea/security-risk-management-uk

September 26-28, 2023

Cloud Expo Asia

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

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

October 11-12, 2023

Les Assises

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

October 11-14, 2023

GITEX

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

October 16-20, 2023

IEEE PAINE Conference

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

October 24-26, 2023

2023 PCI Europe Community Meeting

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

October 24-26

CISO Leaders Summit Thailand

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

November 7, 2023

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

Link back to Table of Contents
The articles have been 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://mena.cs4ca.com/

November 2023

Defense Manufacturing Conference Information

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

December 11-14, 2023

Request for Comments

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

SP 800-207A (Draft) - A Zero Trust Architecture Model for Access Control in Cloud-Native Applications in Multi-Cloud Environments

Source: https://csrc.nist.gov/publications/detail/sp/800-207a/draft

Comments Due: June 7, 2023

NCCoE Releases Preliminary Draft NIST SP 1800-38A, Migration to Post Quantum Cryptography for Public Comment
Source: https://www.nccoe.nist.gov/news-insights/nccoe-releases-preliminary-draft-nist-sp-1800-38a-migration-post-quantum-cryptography

Link back to Table of Contents
The articles have been 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: June 8, 2023

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

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

Comments due: September 30, 2023

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

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

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

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

Source: https://www.federalregister.gov/documents/2022/12/23/2022-27995/national-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/

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

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

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

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

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

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

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

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

Crosswalk AI RMF 1 0 ISO IEC 23894 pdf

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

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

Patches/Advisories

Omron CS/CJ Series

https://www.cisa.gov/news-events/ics-advisories/icsa-23-108-01

APT28 Exploits Known Vulnerability to Carry Out Reconnaissance and Deploy Malware on Cisco Routers

https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-108

Schneider Electric Easy UPS Online Monitoring Software
https://www.cisa.gov/news-events/ics-advisories/icsa-23-108-02

CISA Releases Four Industrial Control Systems Advisories

https://www.cisa.gov/news-events/alerts/2023/04/18/cisa-releases-four-industrial-control-systems-advisories

Review – 2 Advisories and 2 Updates Published – 4-18-23

https://chemical-facility-security-news.blogspot.com/2023/04/review-2-advisories-and-2-updates.html

CISA Releases Malware Analysis Report on ICONICSTEALER

https://www.cisa.gov/news-events/alerts/2023/04/20/cisa-releases-malware-analysis-report-iconicstealer

MAR-10435108-1.v1 ICONICSTEALER

https://www.cisa.gov/news-events/analysis-reports/ar23-110a

INEA ME RTU

https://www.cisa.gov/news-events/ics-advisories/icsa-23-110-01

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

CISA Releases One Industrial Control Systems Advisory

https://www.cisa.gov/news-events/alerts/2023/04/20/cisa-releases-one-industrial-control-systems-advisory

CISA and Partners Release Cybersecurity Best Practices for Smart Cities

https://www.cisa.gov/news-events/alerts/2023/04/19/cisa-and-partners-release-cybersecurity-best-practices-smart-cities

Review - 1 Advisory Published – 4-20-23

https://chemical-facility-security-news.blogspot.com/2023/04/review-1-advisory-published-4-20-23.html

VMware Releases Security Update for Aria Operations for Logs

https://www.cisa.gov/news-events/alerts/2023/04/21/vmware-releases-security-update-aria-operations-logs

Drupal Releases Security Advisory to Address Vulnerability in Drupal Core

https://www.cisa.gov/news-events/alerts/2023/04/21/drupal-releases-security-advisory-address-vulnerability-drupal-core

Oracle Releases Security Updates

https://www.cisa.gov/news-events/alerts/2023/04/21/oracle-releases-security-updates

CISA Adds Three Known Exploited Vulnerabilities to Catalog

https://www.cisa.gov/news-events/alerts/2023/04/21/cisa-adds-three-known-exploited-vulnerabilities-catalog

CISA Releases Two SBOM Documents

https://www.cisa.gov/news-events/alerts/2023/04/21/cisa-releases-two-sbom-documents

Link back to Table of Contents

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

Cisco Releases Security Advisories for Multiple Products

https://www.cisa.gov/news-events/alerts/2023/04/21/cisco-releases-security-advisories-multiple-products

Public ICS Disclosures – Week of 4-15-23

https://chemical-facility-security-news.blogspot.com/2023/04/public-ics-disclosures-week-of-4-15-23.html

Podcasts/Videos

Finding Strength in Weakness – the Benefits of Being Vulnerable – Matt Johansen – ESW #315

Source: https://www.scmagazine.com/podcast-segment/finding-strength-in-weakness-the-benefits-of-being-vulnerable-matt-johansen-esw-315

How to Make the World Quantum Safe – Vadim Lyubashevsky – ESW #315

Source: https://www.scmagazine.com/podcast-segment/how-to-make-the-world-quantum-safe-vadim-lyubashevsky-esw-315

Bringing Useful Quantum Computing to the World – Kayla Lee – ESW #315

Source: https://www.scmagazine.com/podcast-segment/bringing-useful-quantum-computing-to-the-world-kayla-lee-esw-315

Say Easy, Do Hard – Closing the Skills Gap, Part 2 – BSW #303

Source: https://www.scmagazine.com/podcast-segment/say-easy-do-hard-closing-the-skills-gap-part-2-bsw-303

Simply Cyber: 🔴 April 21's Top Cyber News NOW! - Ep 350 on Apple Podcasts

Source: https://podcasts.apple.com/us/podcast/april-21s-top-cyber-news-now-ep-

Link back to Table of Contents

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

350/id1590662228?i=1000610133609

Simply Cyber: 🔴 April 20's Top Cyber News NOW! - Ep 349 on Apple Podcasts

Source: https://podcasts.apple.com/us/podcast/april-20s-top-cyber-news-now-ep-349/id1590662228?i=1000610013115

Simply Cyber: 🔴 April 19's Top Cyber News NOW! - Ep 348 on Apple Podcasts

Source: https://podcasts.apple.com/us/podcast/april-19s-top-cyber-news-now-ep-348/id1590662228?i=1000609677626

Simply Cyber: 🔴 April 18's Top Cyber News NOW! - Ep 347 on Apple Podcasts

Source: https://podcasts.apple.com/us/podcast/april-18s-top-cyber-news-now-ep-347/id1590662228?i=1000609531948

Simply Cyber: 🔴 April 17's Top Cyber News NOW! - Ep 346 on Apple Podcasts

Source: https://podcasts.apple.com/us/podcast/april-17s-top-cyber-news-now-ep-346/id1590662228?i=1000609368203

7MS #568: Lets Play With the 2023 Local Administrator Password Solution!

Source: https://7ms.us/7ms-568-lets-play-with-the-2023-local-administrator-password-solution/

The Hacker Factory: Mastering Cybersecurity Basics and Embracing AI | A Conversation with David Pereira | The Hacker Factory Podcast With Phillip Wylie on Apple Podcasts

Source: https://podcasts.apple.com/us/podcast/mastering-cybersecurity-basics-and-embracing-ai/id1581926992?i=1000610112635

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

Securing Bridges: A Conversation with Chris Roberts @sidragon1 | Securing Bridges Podcast With Alyssa Miller | Episode 38 on Apple Podcasts

Source: https://podcasts.apple.com/us/podcast/a-conversation-with-chris-roberts-sidragon1/id1617553464?i=1000610110437

Forced Entry | TWiT.TV

Source: https://twit.tv/shows/security-now/episodes/919

NO. 378 — AI Resilience Scale, Moloch the Demon, Ukraine Data Leak, and more...

Source: https://danielmiessler.com/podcast/no-378-ai-resilience-scale-moloch-the-demon-ukraine-data-leak-and-more/

Lazarus Group: Breaking down the evolution.

Source: https://thecyberwire.com/podcasts/hacking-humans/240/notes

The Privacy, Security, & OSINT Show – Episode 294 - Preparing for Home Disaster

Source: https://inteltechniques.com/blog/2023/04/21/the-privacy-security-osint-show-episode-294/

318: Tesla workers spy on drivers, and Operation Fox Hunt scams

Source: https://www.smashingsecurity.com/318-tesla-workers-spy-on-drivers-and-operation-fox-hunt-scams/

Ep 1807 | 4.21.23 Daggerfly swarms African telco. EvilExtractor described. Patriotic hacktivism in East Asia. Updates on Russia's hybrid war suggest that cyber warfare has some distinctive challenges.

Source: https://thecyberwire.com/podcasts/daily-podcast/1807/notes

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

Ep 1806 | 4.20.23 Two-step supply-chain attack. Plugging leaks, in both Mother Russia and the Land of the Free and the Home of the Brave. Belarus remains a player in the cyber war.

Source: https://thecyberwire.com/podcasts/daily-podcast/1806/notes

Ep 1805 | 4.19.23 Play ransomware's new tools. A look at what the GRU's been up to. US Air Force opens investigation into alleged leaker's Air National Guard wing. KillNet's new hacker course: "Dark School."

Source: https://thecyberwire.com/podcasts/daily-podcast/1805/notes

Ep 1804 | 4.18.23 Iranian threat actor exploits N-day vulnerabilities. Subdomain hijacking vulnerabilities. The Discord Papers. An update on Russia's NTC Vulkan. And weather reports, not a Periodic Table.

Source: https://thecyberwire.com/podcasts/daily-podcast/1804/notes

Ep 1803 | 4.17.23 Developments in the Discord Papers, including notes on influencers and why they seek influence. Tax season scams. KillNet's selling, but is anyone buying?

Source: https://thecyberwire.com/podcasts/daily-podcast/1803/notes

Risky Biz News: 3CX was a supply chain attack in a supply chain attack

Source: https://risky.biz/RBNEWS136/

Snake Oilers: Socket, Teleport and Mandiant's Purple Team

Source: https://risky.biz/snakeoilers17pt1/

Risky Biz News: Apple's Lockdown Mode wins against iOS zero-day

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

Source: https://risky.biz/RBNEWS135/

Risky Business #702 -- 3CX: It's like SolarWinds, but stupider

Source: https://risky.biz/RB702/

Between Two Nerds: The NCF's Practical Guide to Offensive Cyber Operations

Source: https://risky.biz/BTN32/

Risky Biz News: Israeli spyware vendor QuaDream has allegedly shut down

Source: https://risky.biz/RBNEWS134/

Voices from DARPA Podcast Episode 67: Wireless Power Beaming

Source: https://www.darpa.mil/news-events/2023-04-20

From the Article: "This 13-minute episode of the Voices from DARPA podcast series explores the possibility of an “energy web” that, much like the World Wide Web allows for near-instantaneous communication, could instantly distribute energy from remote, currently untapped sources. DARPA Program Manager Col Paul Calhoun describes his bold POWER program, aimed at leveraging power beaming for energy transport through a multi-path network."

VLOG-204 | The #Semiconductor Memory Innovation

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

How will the Ukraine invasion shape industrial base policy?

Source: https://www.militarytimes.com/video/2023/04/17/how-will-the-ukraine-invasion-shape-industrial-base-policy/

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

Harvard Pilgrim Health Care systems down after ransomware attack - YouTube

Source: https://www.youtube.com/watch%3Fv%3DTD6jl4qJ1Rw

From the Article: "Harvard Pilgrim Health Care said Wednesday that the attack is affecting systems used to service customers and providers."

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 a ByteDance Covered Application
Source: https://www.acq.osd.mil/dpap/dars/opencases/farcasenum/far.pdf

From the Article: “Case Number 2023-010, Part Number 4, 13, 39, 52. Implements OMB Memo M-23-13, No TikTok on Government Devices, and the No TikTok on Government Devices Act which prohibits covered software applications on Government Devices. Status: CAAC Chair sent draft interim FAR rule to OIRA. OIRA reviewing.”

Prohibition on Certain Semiconductor Products and Services

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

From the Article: “Case Number 2023-008, Part Number 4, 52. 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 date extended to 05/17/2023.”

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.

Acquisitions for Foreign Military Sales and Appendix F – Transportation

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

From the Article: “Case Number 2023-D016, Part Number 225.73. Revises DFARS 225.73 to clarify FMS requirements in Appendix F that are necessary to resolve issues associated with the transportation of FMS goods such as lost, misdirected or frustrated shipments with FMS partners. Status: DARC Director tasked Adhoc team to draft proposed DFARS rule. Report due 06/07/2023.

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: Case manager forwarded draft interim rule to DARS Regulatory Control Officer. DARS Regulatory Control Officer reviewing.

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

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 05/17/2023."

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 05/24/2023."

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."

Link back to Table of Contents

Establishing FAR Part 40

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

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

Link back to Table of Contents

of May 2, 2019, America's Cybersecurity Workforce, which directs agencies to incorporate the NICE Framework lexicon, taxonomy and reporting requirements into contracts for information technology and cybersecurity services. Status: DAR staff notified FAR staff of DARC differences from Team report or CAAC suggested changes. 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 05/10/2023."

(EO) DFARS Buy American Act Requirements

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

Link back to Table of Contents

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 05/10/2023."

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 05/31/2023."

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

Link back to Table of Contents

attest to complying with, applicable secure software development requirements in accordance. Status: DARC Director tasked FAR Acquisition Technology & Information Team to draft proposed FAR rule. Report due 04/05/2023."

Enhanced Price Preferences for Critical Components and Critical Items

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

From the Article: "Case Number 2022-004, Part Number 25: Enhanced Price Preferences for Critical Components and Critical Items. Implements Executive Order 14005, Ensuring the Future Is Made in All of America by All of America's Workers to address the identification of critical products and use of enhanced price preferences. Status: DARC Director tasked Staff to draft proposed FAR rule. Due date extended to 05/03/2023."

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

A Vision and Strategy for the NSTC pdf

Source:
https://www.nist.gov/system/files/documents/2023/04/25/A%20Vision%20and%20Strategy%20for%20the%20NSTC.pdf

NSTC Vision Strategy Fact Sheet pdf

Source: https://www.nist.gov/system/files/documents/2023/04/25/NSTC-Vision-Strategy-Fact-Sheet.pdf

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

Semi Europe European Chips Act Trilogue Priorities pdf

Source: https://www.semi.org/sites/semi.org/files/2023-03/SEMI-Europe-European-Chips-Act-Trilogue-Priorities.pdf

Mineral Commodity Summaries 2023

Source: https://pubs.usgs.gov/periodicals/mcs2023/mcs2023.pdf

Reports - Industry

OTORIO - OT security insights survey

Source: https://go.otorio.com/ot-security-survey-04-23

AI language models

Source: https://www.oecd-ilibrary.org/science-and-technology/ai-language-models_13d38f92-en

The State of Security 2023 | Splunk

Source: https://www.splunk.com/en_us/form/state-of-security.html

230414 Bingen Space Assessment pdf

Source: https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-04/230414_Bingen_Space_Assessment.pdf?VersionId=oMsUS8MupLbZi3BISPrqPCKd5jDejZnJ

Top Trends in Cyber Security | Cyber Attacks Trends | M-Trends

Link back to Table of Contents
The articles have been 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.mandiant.com/m-trends

Incident Response Policy Template for CIS Control 17

Source: https://www.cisecurity.org/insights/white-papers/incident-response-policy-template-for-cis-control-17

Does China pose a threat to global rare earth supply chains?

Source: https://chinapower.csis.org/china-rare-earths/

Tracking China's April 2023 Military Exercises around Taiwan | ChinaPower Project

Source: https://chinapower.csis.org/tracking-chinas-april-2023-military-exercises-around-taiwan/

Global Counterspace Capabilities Report

Source: https://swfound.org/counterspace/

New dangers in space - CSIS threat assessment 2023 - RNTF

Source: https://rntfnd.org/2023/04/15/new-dangers-in-space-csis-threat-assessment-2023/

Resilinc's Special Report: Global Semiconductor Industry Review and What to Expect in 2023

Source: https://www.resilinc.com/learning-center/white-papers-reports/resilinc-special-report-global-semiconductor-industry-review-and-what-to-expect-in-2023/?li_fat_id=9722a98f-bc60-42da-90d4-173d99eb6fcd

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

Are Your Passwords in the Green?

Source: https://www.hivesystems.io/blog/are-your-passwords-in-the-green

2023 Annual Risk Report pdf

Source: https://www.everstream.ai/wp-content/uploads/2023/01/2023-Annual-Risk-Report.pdf

White House

Remarks by President Biden at the 2023 Major Economies Forum on Energy and Climate | The White House

Source: https://www.whitehouse.gov/briefing-room/speeches-remarks/2023/04/20/remarks-by-president-biden-at-the-2023-major-economies-forum-on-energy-and-climate/

Remarks by President Biden on his Vision for the Economy | The White House

Source: https://www.whitehouse.gov/briefing-room/speeches-remarks/2023/04/20/remarks-by-president-biden-on-his-vision-for-the-economy/

FACT SHEET: President Biden to Catalyze Global Climate Action through the Major Economies Forum on Energy and Climate | The White House

Source: https://www.whitehouse.gov/briefing-room/statements-releases/2023/04/20/fact-sheet-president-biden-to-catalyze-global-climate-action-through-the-major-economies-forum-on-energy-and-climate/

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/2023/04/17/fact-sheet-biden-harris-administration-announces-new-private-and-public-sector-investments-for-affordable-electric-vehicles/

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

Articles of Interest

LockBit Ransomware Gang Testing First-Ever Ransomware for macOS

Source: https://www.blackhatethicalhacking.com/news/lockbit-ransomware-gang-testing-first-ever-ransomware-for-macos/

From the Article: "The notorious LockBit ransomware gang has recently developed a new set of encryptors designed to target macOS devices for the first time, marking a significant milestone in the history of ransomware attacks."

Additional Sources:
https://securityaffairs.com/144879/cyber-crime/lockbit-encryptor-targets-macos.html

https://www.hackread.com/lockbit-ransomware-attack-mac-devices/

https://www.bankinfosecurity.com/blogs/lockbit-ransomware-tests-taking-bite-out-apple-users-p-3440

https://www.pcmag.com/news/lockbit-ransomware-targets-apple-silicon-macs-for-the-first-time

https://thehackernews.com/2023/04/lockbit-ransomware-now-targeting-apple.html

https://www.theregister.com/2023/04/17/lockbit_ransomware_mac_devices/

https://thehackernews.com/2023/04/lockbit-ransomware-now-targeting-apple.html

https://www.sentinelone.com/blog/lockbit-for-mac-how-real-is-the-risk-of-macos-ransomware/

https://www.securityweek.com/lockbit-ransomware-group-developing-malware-to-encrypt-files-on-macos/

https://www.securitynewspaper.com/2023/04/18/the-new-lockbit-ransomware-for-macos-sounds-scary-but-its-code-is-so-dumb/

https://www.techspot.com/news/98362-lockbit-ransomware-targeting-apple-silicon-early-development.html

https://www.scmagazine.com/news/ransomware/new-lockbit-variant-targets-macos-another-relies-on-conti-source-code

Link back to Table of Contents
The articles have been 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.malwarebytes.com/blog/news/2023/04/lockbit-ransomware-on-mac-should-we-worry

https://www.cysecurity.news/2023/04/lockbit-operators-target-apple-macos.html

https://grahamcluley.com/lockbit-ransomware-for-mac-coming-soon/

https://informationsecuritybuzz.com/apple-macos-devices-now-subject-of-lockbit-ransomware/

https://www.thehindu.com/sci-tech/technology/explained-lockbit-ransomware-and-why-its-targeting-macos/article66766214.ece

https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-april-21st-2023-macs-in-the-crosshairs/

https://www.makeuseof.com/mac-no-longer-safe-from-lockbit-ransomware/

https://www.macworld.com/article/1791783/mac-security-ransomware-macos-hackers-lockbit.html

https://cybersecuritynews.com/first-ever-ransomware/

https://www.darkreading.com/remote-workforce/researchers-discover-first-ever-major-ransomware-targeting-macos

https://bgr.com/tech/infamous-ransomware-gang-is-now-trying-to-target-mac-users/

3CX supply chain attack was the result of a previous supply chain attack, Mandiant says

Source: https://cyberscoop.com/3cx-supply-chain-north-korea/

From the Article: "Hackers linked to North Korea appear to have carried out the first documented instance of a supply chain attack that led to a second, subsequent supply chain attack, researchers at Mandiant concluded in a report released Thursday."

Additional Sources:
https://www.darkreading.com/attacks-breaches/3cx-supply-chain-attack-originated-from-breach-at-another-software-company

https://www.bankinfosecurity.com/north-korean-hackers-chained-supply-chain-hacks-to-

Link back to Table of Contents

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

reach-3cx-a-21714

https://www.infosecurity-magazine.com/news/north-korean-hacker-suspected-3cx/

https://www.welivesecurity.com/2023/04/20/linux-malware-strengthens-links-lazarus-3cx-supply-chain-attack/

https://www.theregister.com/2023/04/20/3cx_supply_chain_attack/

https://thehackernews.com/2023/04/nk-hackers-employ-matryoshka-doll-style.html

https://thehackernews.com/2023/04/lazarus-xtrader-hack-impacts-critical.html

https://thehackernews.com/2023/04/lazarus-group-adds-linux-malware-to.html

https://securityaffairs.com/145073/apt/lazarus-apt-linux-malware-3cx-attack.html

https://krebsonsecurity.com/2023/04/3cx-breach-was-a-double-supply-chain-compromise/

https://www.scmagazine.com/analysis/third-party-risk/mandiant-discovers-another-software-supply-chain-attack-during-3cx-investigation

https://latesthackingnews.com/2023/04/21/3cx-cyber-attack-it-was-the-aftermath-of-another-supply-chain-attack/

https://www.bankinfosecurity.com/north-korean-apt-group-now-deploying-linux-malware-variant-a-21737

https://www.bankinfosecurity.com/symantec-more-xtrader-supply-chain-attacks-uncovered-a-21734

https://www.cysecurity.news/2023/04/linux-malware-set-to-be-deployed-by.html

https://www.bleepingcomputer.com/news/security/3cx-hack-caused-by-trading-software-supply-chain-attack/

https://www.securityweek.com/symantec-north-korean-3cx-hackers-also-hit-critical-infrastructure-orgs/

https://securityaffairs.com/145133/breaking-news/north-korea-apt-3cx-critical-infrastructure.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://gbhackers.com/operation-dreamjob/

Major Mass., NH health insurance provider hit by cyber attack - WCVB-TV

Source: https://www.wcvb.com/article/major-mass-nh-health-insurance-provider-point32health-hit-by-cybersecurity-ransomware-attack/43646234

From the Article: "A major Massachusetts and New Hampshire health insurance company is warning members of a cybersecurity ransomware incident that is affecting systems used to service customers, accounts, brokers and providers, the company said Wednesday. Point32Health, the corporate parent of Harvard Pilgrim Health Care and Tufts Health Plan, said it identified the attack Monday and proactively took some systems offline to contain the threat."

Additional Sources:
https://whdh.com/news/harvard-pilgrim-health-care-parent-company-hit-by-ransomware-attack/

https://www.wmur.com/article/harvard-pilgrim-health-care-ransomware-attack/43647570

https://www.boston.com/news/local-news/2023/04/20/point32health-tufts-harvard-pilgrim-massachusetts-health-insurerance-cybersecurity-attack/

https://news.yahoo.com/harvard-pilgrim-health-care-systems-203428547.html

https://healthitsecurity.com/news/parent-of-2-major-massachusetts-health-insurers-suffers-ransomware-attack

https://www.beckershospitalreview.com/cybersecurity/new-england-health-insurer-dealing-with-ransomware-attack.html

https://www.techtarget.com/searchsecurity/news/365535633/Point32Health-confirms-service-disruption-due-to-ransomware

https://informationsecuritybuzz.com/new-ransomware-attack-hits-insurer-point32health/

https://www.securityweek.com/ransomware-attack-hits-health-insurer-point32health/

https://securityaffairs.com/145183/cyber-crime/point32health-ransomware-attack.html

https://www.jdsupra.com/legalnews/point32health-announces-recent-2701197/

Link back to Table of Contents
The articles have been 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.benefitspro.com/2023/04/20/major-new-england-health-insurer-impacted-by-cybersecurity-attack/

https://www.hipaajournal.com/major-massachusetts-health-insurer-suffers-ransomware-attack/

https://www.boston25news.com/news/local/cybersecurity-incident-impacting-customers-2-big-massachusetts-health-insurers-officials-say/Y43QWGASERGPZKCC7HALC6LHLE/

https://pbn.com/major-mass-health-insurance-company-victim-of-cybersecurity-attack/

Zero Day In Google Chrome Patched: Bug Exploited In The Wild

Source: https://www.scmagazine.com/news/application-security/zero-day-in-google-chrome-patched-bug-exploited-in-the-wild

From the Article: "On Friday Google released an emergency security update for a zero-day vulnerability in its popular Chrome desktop browser that it reported is being actively exploited. The flaw impacts Windows, macOS and Linux versions of the Google Chrome desktop browser prior to build version 112.0.5615.121."

Additional Sources:
https://www.cisecurity.org/advisory/a-vulnerability-in-google-chrome-could-allow-for-arbitrary-code-execution_2023-041

https://www.csoonline.com/article/3693259/google-urges-users-to-update-chrome-to-address-zero-day-vulnerability.html

https://latesthackingnews.com/2023/04/17/google-patched-high-severity-zero-day-flaw-with-latest-chrome-release/

https://www.malwarebytes.com/blog/news/2023/04/update-chrome-now-google-patches-actively-exploited-flaw

https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-google-chrome-could-allow-for-arbitrary-code-execution_2023-043

https://www.theregister.com/2023/04/17/chrome_emergency_patch/

https://gbhackers.com/new-google-chrome-zero-day-bug/

Link back to Table of Contents
The articles have been 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/google-patches-second-chrome-zero-day-vulnerability-of-2023/

https://thehackernews.com/2023/04/google-chrome-hit-by-second-zero-day.html

https://securityaffairs.com/145019/security/google-second-chrome-zero-day-2023.html

https://informationsecuritybuzz.com/google-chrome-hit-second-zero-day-attack/

https://www.2-spyware.com/google-releases-patch-for-yet-another-zero-day-exploit

https://www.sentinelone.com/blog/the-good-the-bad-and-the-ugly-in-cybersecurity-week-16-4/

https://latesthackingnews.com/2023/04/20/google-patched-second-chrome-zero-day-within-a-week/

US and UK agencies warn of Russia-linked APT28 exploiting Cisco router flaws

Source: https://securityaffairs.com/145007/apt/apt28-targets-cisco-networking-equipment.html

From the Article: "Russia-linked APT28 group accesses unpatched Cisco routers to deploy malware exploiting the not patched CVE-2017-6742 vulnerability (CVSS score: 8.8), states a joint report published by the UK National Cyber Security Centre (NCSC), the US National Security Agency (NSA), US Cybersecurity and Infrastructure Security Agency (CISA) and US Federal Bureau of Investigation (FBI)."

Additional Sources:
https://www.csoonline.com/article/3694188/russian-cyber-spy-group-apt28-backdoors-cisco-routers-via-snmp.html

https://www.blackhatethicalhacking.com/news/apt28-hackers-target-cisco-routers-with-custom-malware/

https://blogs.cisco.com/security/threat-actors-exploiting-snmp-vulnerabilities-in-cisco-routers

https://thehackernews.com/2023/04/us-and-uk-warn-of-russian-hackers.html

https://www.securityweek.com/us-uk-russia-exploiting-old-vulnerability-to-hack-cisco-routers/

Link back to Table of Contents

The articles have been 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/attacks-breaches/russian-fancy-bear-apt-exploited-unpatched-cisco-routers-to-hack-us-eu-government-agencies

https://www.ncsc.gov.uk/news/apt28-exploits-known-vulnerability-to-carry-out-reconnaissance-and-deploy-malware-on-cisco-routers

https://thecyberwire.com/podcasts/cisa-cybersecurity-alerts/46/notes

https://www.securityweek.com/cisco-patches-critical-vulnerabilities-in-industrial-network-director-modeling-labs/

https://securityaffairs.com/145108/security/industrial-network-director-and-modeling-labs-critical-flaws.html

https://www.malwarebytes.com/blog/news/2023/04/fancy-bear-known-to-be-exploiting-vulnerability-in-cisco-routers

https://www.infosecurity-magazine.com/news/ncsc-russian-attacks-critical/

https://gbhackers.com/exploiting-vulnerabilities-in-cisco/

https://heimdalsecurity.com/blog/apt28-routers-jaguar-tooth-malware/

https://www.securityweek.com/uk-warns-of-russian-hackers-targeting-critical-infrastructure/

Capita Confirms Data Breach After Ransomware Group Offers to Sell Stolen Information

Source: https://www.securityweek.com/capita-confirms-data-breach-after-ransomware-group-offers-to-sell-stolen-information/

From the Article: "Capita finally confirmed that hackers stole data after the Black Basta ransomware group offered to sell information allegedly stolen from the company."

Additional Sources:
https://www.globaldomainsnews.com/confidential-data-stolen-the-yellow-pages-victims-of-a-cyberattack

https://www.globaldomainsnews.com/confidential-data-stolen-hackers-claim-yellow-pages-cyberattack

Link back to Table of Contents
The articles have been 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://gridinsoft.com/blogs/capita-hacked-black-basta-ransomware/

https://circleid.com/posts/20230420-black-basta-ransomware-dns-investigation-led-to-onenote-and-courier-impersonation

https://www.theregister.com/2023/04/18/capita_breach_gets_worse/

https://www.computerweekly.com/news/365535508/Capita-customer-data-was-stolen-in-March-ransomware-attack

https://techcrunch.com/2023/04/20/outsourcing-giant-capita-fears-customer-data-stolen-during-ransomware-attack/

https://www.scmagazine.com/analysis/ransomware/capita-admits-data-stolen-during-cyberattack

https://www.insurancejournal.com/news/international/2023/04/21/717430.htm

https://www.infosecurity-magazine.com/news/capita-data-taken-march-cyber/

https://www.itechpost.com/articles/117365/20230421/capita-suffers-cyberattack-allegedly-blackbasta-ransomware.htm

https://www.bleepingcomputer.com/news/security/capita-confirms-hackers-stole-data-in-recent-cyberattack/

NCR Hit by Ransomware Attack - PaymentsJournal

Source: https://www.paymentsjournal.com/ncr-hit-by-ransomware-attack/

From the Article: "NCR's data center in Aloha, Hawaii has been hit by a ransomware attack. According to a recent article, NCR reported the issue this past weekend, which impacted its Aloha restaurant point-of-sale product (POS). "

Additional Sources:
https://www.malwarebytes.com/blog/news/2023/04/payment-giants-point-of-sale-outage-caused-by-alphv-ransomware

https://cyberintelmag.com/attacks-data-breaches/aloha-pos-goes-down-for-ncr-following-blackcat-ransomware-attack/

https://www.darkreading.com/ics-ot/aloha-pos-restaurant-software-downed-

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

ransomware-attack

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

https://www.scmagazine.com/news/ransomware/ransomware-strikes-pos-platform-ncr

https://siliconangle.com/2023/04/17/ransomware-attack-causes-outages-payments-giant-ncr/

https://www.securityweek.com/payments-giant-ncr-hit-by-ransomware/

https://www.americanbanker.com/news/ncr-was-hit-with-alphv-ransomware-heres-what-bankers-need-to-know

https://www.cysecurity.news/2023/04/after-blackcat-ransomware-attack-ncr.html

https://gbhackers.com/ncr-global-ransomware-attack/

https://www.hackread.com/blackcat-group-ncr-ransomware-attack/

Microsoft SQL servers hacked to deploy Trigona ransomware - Bleeping Computer

Source: https://www.bleepingcomputer.com/news/security/microsoft-sql-servers-hacked-to-deploy-trigona-ransomware/

From the Article: "After connecting to a server, the threat actors deploy malware dubbed CLR Shell by security researchers from South Korean cybersecurity firm AhnLab who spotted the attacks."

Additional Sources:
https://www.blackhatethicalhacking.com/news/cybercriminals-target-ms-sql-servers-with-trigona-ransomware/

https://securityaffairs.com/145036/cyber-crime/trigona-ransomware-targets-microsoft-sql-servers.html

https://cyberintelmag.com/cloud-security/hacking-of-microsoft-sql-servers-to-spread-trigona-ransomware/

https://www.darkreading.com/remote-workforce/trigona-ransomware-trolling-for-poorly-managed-ms-sql-servers-

Link back to Table of Contents
The articles have been 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://heimdalsecurity.com/blog/trigona-ransomware-deployed-through-vulnerable-microsoft-sql-servers/

https://www.msn.com/en-au/news/techandscience/microsoft-sql-servers-hacked-to-spread-ransomware/ar-AA1a6z80?ocid=Peregrine

https://www.techradar.com/news/microsoft-sql-servers-hacked-to-spread-ransomware

https://www.cybersecurityconnect.com.au/industry/8947-hackers-breach-microsoft-sql-servers-to-deploy-trigona-ransomware

https://cybersecuritynews.com/mimikatz-hacking-tool-to-deploy-trigona-ransomware/

https://www.scmagazine.com/brief/ransomware/microsoft-sql-servers-subjected-to-trigona-ransomware-attacks

New Android Malware Infecting 60 Google Play Apps with Over 100M Installs

Source: https://gbhackers.com/android-malware-60-apps/

From the Article: "Recently, McAfee's Mobile Research Team discovered 'Goldoson,' a new type of Android malware, has crept into the Google Play store through 60 genuine apps, downloaded by a whopping 100 million users."

Additional Sources:
https://www.hackread.com/goldoson-android-malware-100-million-downloads/

https://informationsecuritybuzz.com/goldoson-malware-hits-million-downloads-google-play-store

https://www.infosecurity-magazine.com/news/goldoson-malware-found-60-android/

https://latesthackingnews.com/2023/04/17/goldoson-android-malware-target-korean-users-via-legit-apps/

https://thehackernews.com/2023/04/goldoson-android-malware-infects-over.html

https://www.2-spyware.com/60-google-play-apps-infiltrated-by-malware-affecting-100-million-devices

https://www.darkreading.com/remote-workforce/goldoson-malware-google-play-apps-100m-downloads

Link back to Table of Contents

The articles have been 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.mcafee.com/blogs/other-blogs/mcafee-labs/fakecalls-android-malware-abusing-legitimate-signing-key/

FIN7 and Ex-Conti Cybercrime Gangs Join Forces in Domino Malware Attacks

Source: https://thehackernews.com/2023/04/fin7-and-ex-conti-cybercrime-gangs-join.html

From the Article: "A new strain of malware developed by threat actors likely affiliated with the FIN7 cybercrime group has been put to use by the members of the now-defunct Conti ransomware gang, indicating collaboration between the two crews."

Additional Sources:
https://www.securityweek.com/new-domino-malware-linked-to-fin7-group-ex-conti-members/

https://securityaffairs.com/144943/cyber-crime/relationships-fin7-conti-ransomware.html

https://www.malwarebytes.com/blog/news/2023/04/malware-authors-join-forces-and-target-organisations-with-domino-backdoor

https://www.cysecurity.news/2023/04/domino-backdoor-malware-created-by-fin7.html

https://gbhackers.com/domino/

https://heimdalsecurity.com/blog/new-domino-malware-strain/

https://www.darkreading.com/attacks-breaches/fin7-former-conti-gang-members-collaborate-domino-malware

Global Spyware Attacks Spotted Against Both New & Old iPhones

Source: https://www.darkreading.com/mobile/global-spyware-attacks-spotted-new-old-iphones-global-attacks

From the Article: "Campaigns that wielded NSO Group's Pegasus against high-risk users over a six-month period demonstrate the growing sophistication and relentless nature of spyware actors."

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

Additional Sources:
https://thehackernews.com/2023/04/nso-group-used-3-zero-click-iphone.html

https://thecyberwire.com/newsletters/privacy-briefing/5/75

https://www.infosecurity-magazine.com/news/pegasus-spyware-found-high-risk/

https://www.scmagazine.com/news/application-security/nso-group-iphone-zero-click-exploit

https://www.schneier.com/blog/archives/2023/04/new-zero-click-exploits-against-ios.html

https://www.darkreading.com/attacks-breaches/nso-group-back-business-3-new-ios-zero-click-exploits

https://www.securityweek.com/nso-group-used-at-least-3-ios-zero-click-exploits-in-2022-citizen-lab/

AI tools like ChatGPT expected to fuel BEC attacks

Source: https://www.helpnetsecurity.com/2023/04/17/bec-attacks-language-attack-vector/

From the Article: "Across all BEC attacks seen over the past year, 57% relied on language as the main attack vector to get them in front of unsuspecting employees, according to Armorblox."

Additional Sources:
https://www.cysecurity.news/2023/04/chatgpts-cybersecurity-threats-and-how.html

https://unit42.paloaltonetworks.com/chatgpt-scam-attacks-increasing/

https://blog.knowbe4.com/report-gpt4-aid-both-sides-of-cybersecurity-battle

https://www.infosecurity-magazine.com/news/phishing-surge-threat-actors-ai/

https://www.scmagazine.com/news/emerging-technology/attackers-using-ai-to-enhance-conversational-scams-over-mobile-devices

https://www.theregister.com/2023/04/20/ai_defenders_ready_to_foil/

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

Trojanized Installers Used to Distribute Bumblebee Malware - Infosecurity Magazine

Source: https://www.infosecurity-magazine.com/news/trojanized-installers-distribute/

From the Article: "Secureworks' Counter Threat Unit (CTU) analyzed the findings in a report published on Thursday, saying the infection chain for several of these attacks relied on a malicious Google Ad that sent users to a fake download page via a compromised WordPress site."

Additional Sources:
https://www.bleepingcomputer.com/news/security/google-ads-push-bumblebee-malware-used-by-ransomware-gangs/

https://therecord.media/bumblebee-malware-uses-fake-chatgpt-zoom-installers

https://www.infosecurity-magazine.com/news/trojanized-installers-distribute/

https://www.infosecurity-magazine.com/news/chatgpt-related-malicious-urls-rise/

Fortra Hacker Installed Tools on Victim Machines

Source: https://www.bankinfosecurity.com/fortra-hacker-installed-tools-on-victim-machines-a-21724

From the Article: "Hackers who turned a zero-day in Fortra's GoAnywhere software into a bonanza of ransomware attacks for Russian-speaking extortion group Clop first penetrated the company's software in January. "

Additional Sources:
https://thehackernews.com/2023/04/fortra-sheds-light-on-goanywhere-mft.html

https://www.securityweek.com/fortra-completes-investigation-into-goanywhere-zero-day-incident

https://techcrunch.com/2023/04/19/nationsbenefits-confirms-thousands-had-personal-data-stolen-in-fortra-breach/

https://www.hipaajournal.com/healthcare-ransomware-attacks-threaten-up-to-30-of-operating-income/

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

CommScope Holding Company, Inc. Experiences Ransomware Attack and Possibly Data ...

Source: https://www.jdsupra.com/legalnews/commscope-holding-company-inc-2884156/

From the Article: "On April 17, 2023, reports began to emerge about a possible CommScope Holding Company, Inc. data breach following what the company believes to have been a ransomware attack. "

Additional Sources:
https://infotechlead.com/security/commscope-faces-ransomware-attack-77937

https://www.cysecurity.news/2023/04/commscope-ransomware-attack-exposes.html

https://heimdalsecurity.com/blog/commscope-hit-by-ransomware/

https://www.business-standard.com/technology/tech-news/hackers-release-sensitive-information-after-ransomware-attack-on-commscope-123042000677_1.html

GuidePoint Research and Intelligence Team's (GRIT) 2023 Q1 Ransomware Report ...

Source: https://www.businesswire.com/news/home/20230420005030/en/GuidePoint-Research-and-Intelligence-Team%E2%80%99s-GRIT-2023-Q1-Ransomware-Report-Highlights-a-25-Increase-in-Public-Ransomware-Victims-Compared-to-Q4-2022

From the Article: "GuidePoint Security, a cybersecurity solutions leader enabling organizations to make smarter decisions and minimize risk, today announced the release of GuidePoint Research and Intelligence Team’s (GRIT) Q1 2023 Ransomware Report. This report is based on data obtained from publicly available resources, including threat groups themselves, and insight into the ransomware threat landscape."

Additional Sources:
https://securityboulevard.com/2023/04/quarterly-grit-ransomware-report-q1-2023/

https://us.acrofan.com/detail.php?number=816290

https://betanews.com/2023/04/20/number-of-ransomware-victims-increases-by-25-percent/

Link back to Table of Contents
The articles have been 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://industrialcyber.co/reports/guidepoint-ransomware-analysis-detects-quarterly-rise-in-novel-coercive-tactics-as-raas-ecosystem-evolves/

Ransomware group behind Oakland attack strengthens capabilities with new tools, researchers say

Source: https://cyberscoop.com/play-ransomware-custom-tools-data-gathering/

From the Article: "The PLAY ransomware group — responsible for a recent attack on the city of Oakland, California, that forced a state of emergency — has developed two new custom data-gathering tools that allow it to more effectively carry out already crippling digital extortion campaigns, researchers said Wednesday."

Additional Sources:
https://thecyberwire.com

https://duo.com/decipher/play-ransomware-attacks-utilize-new-custom-tools

https://www.securitynewspaper.com/2023/04/20/found-grixba-vss-copying-tools-in-network-means-your-network-will-be-hacked-soon-by-ransomware/

https://thecyberwire.com/newsletters/daily-briefing/12/75

UK NCSC warns of new class of Russian cyber adversary threatening critical infrastructure

Source: https://www.csoonline.com/article/3693773/uk-ncsc-warns-of-new-class-of-russian-cyber-adversary-threatening-critical-infrastructure.html

From the Article: "The UK National Cyber Security Centre (NCSC) has issued an alert to critical national infrastructure (CNI) organisations warning of an emerging threat from state-aligned groups, particularly those sympathetic to Russia's invasion of Ukraine."

Additional Sources:
https://heimdalsecurity.com/blog/russian-hacktivists-shifting-interest-to-business-sector-uk-cyber-agency-warns/

https://industrialcyber.co/critical-infrastructure/russian-groups-could-launch-destructive-and-disruptive-attacks-on-critical-national-infrastructure-uk-ncsc-warns/

Link back to Table of Contents
The articles have been 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/cyberuk23-five-takeaways-uk-cyber

https://www.infosecurity-magazine.com/news/threat-irresponsible-use-hacking/

Ukraine remains Russia's biggest cyber focus in 2023

Source: https://blog.google/threat-analysis-group/ukraine-remains-russias-biggest-cyber-focus-in-2023/

From the Article: "Google's Threat Analysis Group shares first quarter cyber updates on the threat landscape from the war in Ukraine."

Additional Sources:
https://www.bankinfosecurity.com/ukraine-facing-phishing-attacks-information-operations-a-21704

https://www.bankinfosecurity.com/cyber-experts-predict-more-harmful-cyberattacks-in-ukraine-a-21726

https://thehackernews.com/2023/04/google-tag-warns-of-russian-hackers.html

https://www.techcentral.ie/off-the-shelf-ransomware-is-spurring-a-new-era-in-the-ukraine-war/

Ransomware gangs abuse Process Explorer driver to kill security software

Source: https://www.bleepingcomputer.com/news/security/ransomware-gangs-abuse-process-explorer-driver-to-kill-security-software/

From the Article: "Threat actors use a new hacking tool dubbed AuKill to disable Endpoint Detection & Response (EDR) Software on targets' systems before deploying backdoors and ransomware in Bring Your Own Vulnerable Driver (BYOVD) attacks."

Additional Sources:
https://www.darkreading.com/attacks-breaches/aukill-malware-hunts-kills-edr-processes

https://gbhackers.com/aukill-malware-windows-systems/

https://duo.com/decipher/outdated-windows-driver-used-in-ransomware-attacks

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

New QBot Banking Trojan Campaign Hijacks Business Emails to Spread Malware

Source: https://thehackernews.com/2023/04/new-qbot-banking-trojan-campaign.html

From the Article: "A new QBot malware campaign is leveraging hijacked business correspondence to trick unsuspecting victims into installing the malware, new findings from Kaspersky reveal."

Additional Sources:
https://www.csoonline.com/article/3693769/new-qbot-campaign-delivers-malware-by-hijacking-business-emails.html

https://cyberintelmag.com/malware-viruses/business-emails-hijacked-by-new-qbot-banking-trojan-campaign-for-distributing-malware/

https://securityaffairs.com/144927/cyber-crime/qbot-campaign-april-2023.html

WordPress Security: 1 Million WordPress Sites Hacked via Zero-Day Plug-in Bugs

Source: https://www.cysecurity.news/2023/04/wordpress-security-1-million-wordpress.html

From the Article: "A campaign that utilizes several WordPress plug-ins and theme vulnerabilities to inject malicious code into websites, including a sizable number of zero-days, has infected at least 1 million WordPress-sponsored websites. "

Additional Sources:
https://www.securityweek.com/abandoned-wordpress-plugin-abused-for-backdoor-deployment/

https://securityaffairs.com/145146/hacking/eval-php-wordpress-plugin-abused-backdoor.html

https://heimdalsecurity.com/blog/cybercriminals-abusing-an-abandoned-wordpress-plugin-for-malicious-code-injection/

Halcyon Secures $50M Funding for Anti-Ransomware Protection Platform

Source: https://www.securityweek.com/halcyon-secures-50m-funding-for-anti-

Link back to Table of Contents

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

ransomware-protection-platform/

From the Article: "Texas startup scores financing to build an AI-powered anti-ransomware engine to help organizations ward off data-extortion attacks."

Additional Sources:
https://www.verdict.co.uk/cybersecurity-startup-halcyon-50m-funding/

https://siliconangle.com/2023/04/20/cybersecurity-startup-halcyon-raises-50m-assist-development-cyber-resilience-platform/

https://techcrunch.com/2023/04/20/halcyon-lands-large-investment-to-defend-against-ransomware/

Israeli Spyware Vendor QuaDream to Shut Down Following Citizen Lab and Microsoft Expose

Source: https://thehackernews.com/2023/04/israeli-spyware-vendor-quadream-to-shut.html

From the Article: "Israeli spyware vendor QuaDream is allegedly shutting down its operations in the coming days, less than a week after its hacking toolset was exposed by Citizen Lab and Microsoft."

Additional Sources:
https://securityaffairs.com/144935/security/quadream-is-shutting-down.html

https://www.hackread.com/quadream-israeli-iphone-hacking-spyware-shut-down/

https://www.theregister.com/2023/04/19/quadream_nso_spyware/

EU strikes €43 billion deal to boost semiconductor chip production

Source: https://www.euronews.com/next/2023/04/19/eu-strikes-deal-to-boost-semiconductor-chip-production

From the Article: "The European Parliament and EU member states reached an agreement on Tuesday on how to boost the supply of semiconductors in Europe, as the bloc races to reduce its dependency on Asian suppliers."

Link back to Table of Contents

Additional Sources:
https://www.digitimes.com/news/a20230419VL211/eu-ic-manufacturing.html

https://www.semi.org/en/news-media-press-releases/semi-press-releases/semi-applauds-provisional-agreement-reached-in-eu-chips-act-trilogue-negotiations

https://www.euronews.com/next/2023/04/19/eu-strikes-deal-to-boost-semiconductor-chip-production

Over half of Indian IT professionals report increase in ransomware attacks in the past 12 months

Source: https://www.techcircle.in/2023/04/19/over-half-of-indian-it-professionals-report-increase-in-ransomware-attacks-in-the-past-12-months-study/

From the Article: "In India, more than half (52%) of IT professionals reported an increase in ransomware attacks in the past 12 months, higher than the global figure of 48%, in a research report published on Tuesday. Surprisingly, less than half (48%) of enterprises surveyed in India have a formal ransomware plan, the report said. "

Additional Sources:
https://ciosea.economictimes.indiatimes.com/news/security/increase-in-ransomware-attacks-and-human-error-main-cause-of-cloud-data-breaches-report/99599770

https://www.business-standard.com/technology/tech-news/ransomware-attacks-human-error-main-cause-of-cloud-data-breaches-report-123041900719_1.html

https://timesofindia.indiatimes.com/city/hyderabad/over-50-techies-in-india-saw-jump-in-ransomware-attacks/articleshow/99652538.cms

Nation-state threat actor Mint Sandstorm refines tradecraft to attack high-value targets

Source: https://www.microsoft.com/en-us/security/blog/2023/04/18/nation-state-threat-actor-mint-sandstorm-refines-tradecraft-to-attack-high-value-targets/

From the Article: "Over the past several months, Microsoft has observed a mature subgroup of Mint Sandstorm, an Iranian nation-state actor previously tracked as PHOSPHORUS, refining its tactics, techniques, and procedures (TTPs)."

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://heimdalsecurity.com/blog/iranian-hackers-target-u-s-energy-and-transit-systems/

https://www.scmagazine.com/news/vulnerability-management/apt-mint-sandstorm-poc-hacks

https://thehackernews.com/2023/04/iranian-government-backed-hackers.html

TSMC may post single-digit revenue drop in 2023

Source: https://www.digitimes.com/news/a20230418PD214/apple-tsmc.html

From the Article: "Chip orders for the next iPhones will be key in determining if TSMC can meet its modest revenue growth target for 2023, despite the fact that the pure-play foundry may see a single-digit revenue decline this year, according to sources at semiconductor..."

Additional Sources:
https://www.digitimes.com/news/a20230420PD215/ic-design-mediatek-tsmc.html

https://www.digitimes.com/news/a20230417PD200/asml-euv-semiconductor-equipment-tsmc.html

https://www.digitimes.com/news/a20230413PD202/capacity-expansion-chips+components-foundry-taiwan-ic-design-tsmc.html

WhatsApp Includes a New Device Verification Feature to Counter Account Takeover Attacks

Source: https://cyberintelmag.com/malware-viruses/whatsapp-includes-a-new-device-verification-feature-to-counter-account-takeover-attacks/

From the Article: "On Thursday, the popular instant messaging service WhatsApp unveiled a new account verification feature that will prevent malware from affecting users' accounts while it is active on their mobile devices."

Additional Sources: https://www.bankinfosecurity.com/whatsapp-signal-preview-uk-exit-over-threat-to-encryption-a-21699

https://www.infosecurity-magazine.com/news/online-safety-bill-threatens-user/

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

CISA Adds Chrome, macOS Bugs to Known Exploited Vulnerabilities Catalog

Source: https://www.securityweek.com/cisa-adds-chrome-macos-bugs-to-known-exploited-vulnerabilities-catalog/

From the Article: "CISA has added two vulnerabilities to its 'must patch' list, including a recently fixed Chrome flaw and a macOS flaw exploited by the DazzleSpy malware."

Additional Sources:
https://securityaffairs.com/144967/security/cisa-chrome-macos-known-exploited-vulnerabilities-catalog.html

https://securityaffairs.com/145139/security/known-exploited-vulnerabilities-catalog-minio-papercut-and-chrome.html

Daggerfly Cyberattack Campaign Strikes African Telecom Providers

Source: https://informationsecuritybuzz.com/daggerfly-cyberattack-campaign-strikes-african-telecom-providers/

From the Article: "African Telecom Service Providers Targeted by Daggerfly Cyberattack Campaign. Recently, the Daggerfly cyberattack campaign, aimed at numerous institutions worldwide, shocked the cybersecurity community."

Additional Sources:
https://www.infosecurity-magazine.com/news/daggerfly-apt-targets-african/

https://thehackernews.com/2023/04/daggerfly-cyberattack-campaign-hits.html

CISA Releases Two SBOM Documents | CISA

Source: https://www.cisa.gov/news-events/alerts/2023/04/21/cisa-releases-two-sbom-documents

From the Article: "CISA released two community-drafted documents around Software Bill of Materials (SBOM): Types of SBOM documents and Minimum Requirements for Vulnerability Exploitability eXchange (VEX). "

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.tenable.com/blog/cybersecurity-snapshot-the-latest-on-supply-chain-security-sbom-distribution-open-source-flaws

https://industrialcyber.co/cisa/cisa-releases-sbom-sharing-lifecycle-report-covering-different-parties-and-phases/

YouTube Videos Using Highly Evasive Loader to Distribute Aurora Stealer Malware

Source: https://cyberintelmag.com/malware-viruses/youtube-videos-using-highly-evasive-loader-to-distribute-aurora-stealer-malware/

From the Article: "The inner workings of the very evasive loader known as “in2al5d p3in4er” (read: invalid printer), which is used to distribute the Aurora information-stealing malware, have been described by cybersecurity researchers."

Additional Sources:
https://thehackernews.com/2023/04/youtube-videos-distributing-aurora.html

https://www.csoonline.com/article/3693909/hard-to-detect-malware-loader-distributed-via-ai-generated-youtube-videos.html

Vice Society Ransomware Using Stealthy PowerShell Tool for Data Exfiltration

Source: https://thehackernews.com/2023/04/vice-society-ransomware-using-stealthy.html

From the Article: "Threat actors associated with the Vice Society ransomware gang have been observed using a bespoke PowerShell-based tool to fly under the radar and automate the process of exfiltrating data from compromised networks."

Additional Sources:
https://cybersecuritynews.com/vice-society-ransomware-2/

https://securityaffairs.com/144898/breaking-news/vice-society-powershell-tool-exfiltration.html

GhostToken Flaw Could Let Attackers Hide Malicious Apps in Google Cloud Platform

Source: https://thehackernews.com/2023/04/ghosttoken-flaw-could-let-attackers.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: "Cybersecurity researchers have disclosed details of a now-patched zero-day flaw in Google Cloud Platform (GCP) that could have enabled threat actors to conceal an unremovable, malicious application inside a victim's Google account."

Additional Sources:
https://informationsecuritybuzz.com/ghosttoken-gcp-bug-gives-entry-attackers-google-accounts/

https://www.securityweek.com/google-cloud-platform-vulnerability-led-to-stealthy-account-backdoors/

Some NH restaurants affected by nationwide ransomware attack on point-of-sale system

Source: https://news.yahoo.com/nh-restaurants-affected-nationwide-ransomware-225334596.html

From the Article: "Dozens of establishments across New Hampshire have been impacted by a nationwide ransomware attack."

Additional Sources:
http://biz.manchesterinklink.com/ncr-ransomware-attack-is-crippling-for-some-nh-restaurants/

https://www.wmur.com/article/new-hampshire-restaurants-ransomware-attack-42323/43678857

CyberMaxx Releases First Quarter Ransomware Research Report - Benzinga

Source: https://www.benzinga.com/pressreleases/23/04/n31934070/cybermaxx-releases-first-quarter-ransomware-research-report

From the Article: " CyberMaxx, Inc., a tech-enabled cybersecurity services company, today released the first quarter 2023 edition of its Ransomware Research Report. The cyber research team at CyberMaxx conducts routine threat research independent of client engagements in order to help foster collective intelligence among the cybersecurity community."

Additional Sources:
https://finance.yahoo.com/news/cybermaxx-releases-first-quarter-ransomware-

Link back to Table of Contents

130000495.html

https://www.prnewswire.com/news-releases/cybermaxx-releases-first-quarter-ransomware-research-report-301803524.html

Russian national sentenced to time served for committing money laundering for the Ryuk ransomware operation

Source: https://securityaffairs.com/145029/cyber-crime/russian-national-sentenced-money-laundering-ryuk-ransomware.html

From the Article: "Russian national Denis Dubnikov (30) has been sentenced to time served for committing money laundering for the Ryuk ransomware group. The man was also ordered to pay $2,000 in restitution. "

Additional Sources:
https://coingeek.com/no-prison-time-for-ryuk-ransomware-gang-broker-after-guilty-plea/

https://www.securityweek.com/russian-man-who-laundered-money-for-ryuk-ransomware-gang-sentenced/

Experts disclosed two critical flaws in Alibaba cloud database services

Source: https://securityaffairs.com/145061/hacking/brokensesame-alibaba-cloud-flaws.html

From the Article: "Researchers from cloud security firm Wiz discovered two critical flaws, collectively dubbed BrokenSesame, in Alibaba Cloud's ApsaraDB RDS for PostgreSQL and AnalyticDB for PostgreSQL."

Additional Sources:
https://gbhackers.com/accidental-write-permissions-in-alibaba-postgresql/

https://thehackernews.com/2023/04/two-critical-flaws-found-in-alibaba.html

Cigent Unveils Storage Device With Ransomware Prevention Functions - ExecutiveBiz

Source: https://blog.executivebiz.com/2023/04/cigent-unveils-storage-device-with-ransomware-prevention-functions/

Link back to Table of Contents

The articles have been 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: "Cigent Secure SSD+ comes with an artificial intelligence microprocessor with machine learning that works to stop ransomware and safeguard data on the device from being encrypted or stolen by constantly monitoring disk activity, the company said Wednesday."

Additional Sources:
https://www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware/cigent-touts-new-ssd-drive-to-fight-ransomware-at-the-storage-level/

https://www.prweb.com/releases/cigent_announces_first_ever_self_defending_storage_device_with_built_in_ransomware_prevention/prweb19290112.htm

HHS unveils Cybersecurity Resiliency Landscape Analysis, as cyber attacks become more sophisticated

Source: https://industrialcyber.co/medical/hhs-unveils-cybersecurity-resiliency-landscape-analysis-as-cyber-attacks-become-more-sophisticated/

From the Article: "The U.S. Department of Health and Human Services (HHS) 405(d) Program conducted a Hospital Resiliency Landscape Analysis that reviewed active threats attacking hospitals and the cybersecurity capabilities of hospitals. "

Additional Sources:
https://industrialcyber.co/medical/hhs-hicp-document-improves-cybersecurity-posture-focuses-on-zero-trust-defense-in-depth-strategies/

https://www.nextgov.com/cybersecurity/2023/04/hhs-launches-new-cybersecurity-awareness-resources/385271/

Novel Technique Exploits Kubernetes RBAC to Create Backdoors

Source: https://www.bankinfosecurity.com/novel-technique-exploits-kubernetes-rbac-to-backdoor-clusters-a-21738

From the Article: "Threat actors are exploiting Kubernetes Role-Based Access Control in the wild to create backdoors and to run cryptocurrency miners. Researchers observed a recent campaign that targeted at least 60 Kubernetes clusters by deploying DaemonSets to hijack and steal resources from the victims' clusters."

Link back to Table of Contents
The articles have been 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://gbhackers.com/kubernetes-rbac/

https://thehackernews.com/2023/04/kubernetes-rbac-exploited-in-large.html

Hackers Selling ChatGPT Premium Accounts On the Dark Web

Source: https://gbhackers.com/hackers-selling-chatgpt-premium-accounts/

From the Article: "As more stolen ChatGPT Premium accounts are traded, cybercriminals can circumvent OpenAI's geofencing restrictions and gain unrestricted access to ChatGPT, according to Check Point Research (CPR)."

Additional Sources:
https://gbhackers.com/chatgpt-account-takeover-bug/

https://www.cysecurity.news/2023/04/chatgpt-threat-to-privacy.htm

Phishing Email Volume Doubles in Q1 as the use of Malware in Attacks Slightly Declines

Source: https://blog.knowbe4.com/phishing-email-volume-doubles

From the Article: "New data shows that cybercriminals started this year off with a massive effort using new techniques and increased levels of attack sophistication."

Additional Sources:
https://www.itsecurityguru.org/2023/04/19/knowbe4-q1-phishing-report-reveals-it-and-online-services-emails-drive-dangerous-attack-trend/

https://www.darkreading.com/vulnerabilities-threats/knowbe4-phishing-test-results-reveal-it-and-online-services-emails-drive-dangerous-attack-trend-

Ransomware attacks increased 91% in March, as threat actors find new vulnerabilities

Source: https://www.techrepublic.com/article/ransomware-attacks-increased-march/

From the Article: "Ransomware attacks skyrocketed last month according to the new monthly cybersecurity report by NCC Group. New threat group Cl0p is behind the increase as it exploited vulnerabilities in GoAnywhere file transfer manager."

Link back to Table of Contents

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

Additional Sources:
https://www.scmagazine.com/brief/ransomware/record-high-monthly-ransomware-attack-prevalence-recorded-in-march

https://www.cysecurity.news/2023/04/ransomware-attacks-surge-in-march-2023.html

CSC exposes subdomain hijacking vulnerabilities. LockBit group gearing up to target Apple products. Vice Society using "living off the land" techniques for exfiltration.

Source: https://thecyberwire.com/podcasts/research-briefing/164/notes

From the Article: "CSC exposes subdomain hijacking vulnerabilities. LockBit group gearing up to target Apple products. Vice Society using "living off the land" techniques for exfiltration. "

Additional Sources: https://thecyberwire.com/newsletters/research-briefing/5/16

The Car Thieves Using Tech Disguised Inside Of Old Nokia Phones And Bluetooth Speakers

Source: https://www.vice.com/en/article/v7beyj/car-thieves-tech-hidden-old-nokia-phones-bluetooth-speakers-emergency-engine-start-keyless

From the Article: "A man sitting in the driver's seat of a Toyota is repeatedly tapping a button next to the steering wheel. A red light flashes—no luck, the engine won't start. He doesn't have the key. In response, the man pulls up an usual tool: a Nokia 3310 phone."

Additional Sources:
https://gbhackers.com/hackers-using-old-nokia-3310-phone-to-start-car/

For 'resilient' casino giant, a new hurdle: A ransomware attack | London Free Press

Source: https://lfpress.com/news/local-news/for-resilient-casino-giant-a-new-hurdle-a-ransomware-attack

From the Article: "A ransomware cybersecurity attack that's shut down Gateway Casino and Entertainment is a blow to the business here and nationwide as it continues to

emerge from the pandemic, one gambling industry official says."

Additional Sources:
https://www.casino.org/news/gateway-casinos-confirms-cyberattack-on-ontario-it-infrastructure/

Chinese App Uses Android Flaw To Spy On Users, CISA Warns

Source: https://informationsecuritybuzz.com/chinese-app-uses-android-flaw-spy-users-cisa-warns/

From the Article: "The Chinese app for e-commerce Pinduoduo is suspected of having used a high-severity Android vulnerability as a zero-day to spy on its users, in line with the U.S. Cybersecurity and Infrastructure Security Agency (CISA)."

Additional Sources:
https://www.infosecurity-magazine.com/news/cisa-patch-bug-exploited-chinese/

Cisco and VMware Release Security Updates to Patch Critical Flaws in their Products

Source: https://thehackernews.com/2023/04/cisco-and-vmware-release-security.html

From the Article: "Cisco and VMware have released security updates to address critical security flaws in their products that could be exploited by malicious actors to execute arbitrary code on affected systems."

Additional Sources:
https://informationsecuritybuzz.com/cisco-and-vmware-issues-security-updates-for-critical-flaws/

CVE-2023-20864: VMware Aria Operations for Logs Deserialization Vulnerability

Source: https://www.tenable.com/blog/cve-2023-20864-vmware-aria-operations-for-logs-deserialization-vulnerability

From the Article: "On April 20, VMware published an advisory (VMSA-2023-0007) to address two vulnerabilities in VMware Aria Operations for Logs, formerly known as vRealize Log Insight, a centralized log management solution."

Link back to Table of Contents

Additional Sources:
https://securityaffairs.com/145087/security/critical-flaw-vmware-vrealize.html

QueueJumper: Critical Unauthenticated RCE Vulnerability in MSMQ Service

Source: https://research.checkpoint.com/2023/queuejumper-critical-unauthorized-rce-vulnerability-in-msmq-service/

From the Article: "Check Point Research recently discovered three vulnerabilities in the “Microsoft Message Queuing” service, commonly known as MSMQ. These vulnerabilities were disclosed to Microsoft and patched in the April Patch Tuesday update. "

Additional Sources:
https://blog.checkpoint.com/security/watch-out-critical-unauthorized-rce-vulnerability-in-msmq-service/

Chinese hacking group APT41 caught using Google tool for data theft

Source: https://www.blackhatethicalhacking.com/news/chinese-hacking-group-apt41-caught-using-google-tool-for-data-theft/

From the Article: "Chinese state-sponsored hacking group APT41, also known as HOODOO, has been caught using Google’s open-source GC2 (Google Command and Control) red teaming tool in data theft attacks against a Taiwanese media company and an Italian job search website."

Additional Sources:
https://www.darkreading.com/vulnerabilities-threats/apt41-taps-google-red-teaming-tool-targeted-info-stealing-attacks

Major US CFPB Data Breach Caused by Employee

Source: https://www.darkreading.com/attacks-breaches/major-us-cfpb-data-breach-employee

From the Article: "The sensitivity of the personal information involved in the breach has yet to be determined by agency officials, but it affects 256,000 consumers."

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

Additional Sources:
https://www.scmagazine.com/brief/data-security/nearly-256k-impacted-by-cfpb-data-breach

Criminal Records Service is Still Disrupted 4 Weeks after Hack!

Source: https://www.cybernewsgroup.co.uk/criminal-records-service-is-still-disrupted-4-weeks-after-hack/

From the Article: "The Acro Criminal Records Office provides records to police, exchanges them internationally & processes certificates for people wishing to work with children or gain emigration visas."

Additional Sources:
https://www.cysecurity.news/2023/04/criminal-records-service-still-not.html

A Corporate Secret is not Destroyed, it's Discarded: Threat of Old Routers

Source: https://www.cysecurity.news/2023/04/a-corporate-secret-is-not-destroyed-its.html

From the Article: "Many business network environments probably experience the process of removing a defunct router from a rack and accommodating a shiny refurbished replacement now and then. "

Additional Sources: https://www.welivesecurity.com/2023/04/18/discarded-not-destroyed-old-routers-reveal-corporate-secrets/

Oracle Patch Tuesday April 2023 Security Update Review

Source: https://blog.qualys.com/vulnerabilities-threat-research/patch-tuesday/2023/04/19/oracle-patch-tuesday-april-2023-security-update-review

From the Article: "Oracle has released the second quarterly edition of Critical Patch Update, which contains a group of patches for 433 security vulnerabilities. Some of the vulnerabilities addressed this month impact various products. These patches address vulnerabilities in Oracle code and third-party components included in Oracle products. "

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.cisecurity.org/advisory/oracle-quarterly-critical-patches-issued-april-18-2023_2023-042

Five Eye nations release new guidance on smart city cybersecurity

Source: https://www.csoonline.com/article/3694149/five-eye-nations-release-new-guidance-on-smart-city-cybersecurity.html

From the Article: "New guidance, Cybersecurity Best Practices for Smart Cities, wants to raise awareness among communities and organizations implementing smart city technologies that these beneficial technologies can also have potential vulnerabilities."

Additional Sources:
https://www.securityweek.com/five-eyes-agencies-issue-cybersecurity-guidance-for-smart-cities/

OpenSSF Adds Software Supply Chain Tracks to SLSA Framework

Source: https://www.darkreading.com/dr-tech/openssf-adds-software-supply-chain-tracks-to-slsa-framework

From the Article: "The Open Source Security Foundation's SLSA v1.0 release is an important milestone in improving software supply chain security and providing organizations with the tools they need to protect their software."

Additional Sources:
https://www.csoonline.com/article/3693693/openssf-releases-slsa-v1-0-adds-software-supply-chain-specific-tracks.html

Poorly Set Server, Human Error Blamed for DC Health Breach

Source: https://www.bankinfosecurity.com/poorly-set-server-human-error-blamed-for-dc-health-breach-a-21710

From the Article: "House Oversight Committee members on Thursday called for the firing of whoever caused the DC Health Benefit Exchange breach and exposed the personal information of Congress members on a dark web forum. "

Additional Sources: https://www.securityweek.com/house-committee-hears-testimony-

Link back to Table of Contents

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

on-dc-health-data-breach/

Killnet Ostracizes Leader of Anonymous Russia, Adding New Chapter to Pro-Kremlin Hacktivist Drama

Source: https://flashpoint.io/blog/killnet-anonymous-russia-pro-kremlin-hacktivism/

From the Article: "The world of pro-Kremlin hacktivists may be shaken up by the latest move of Killmilk, the founder and de facto leader of the Killnet group who announced on April 15 that he had to “make a difficult decision” and reveal the real-life identity of “Raty”, the head of Anonymous Russia, a group that initially conducted distributed denial of service (DDoS) attacks in Ukraine, and later joined several Killnet campaigns, becoming an associated group more tightly integrated with Killnet’s command structure."

Additional Sources:
https://www.darkreading.com/threat-intelligence/killnet-boss-rival-leader-kremlin-hacktivist-beef

Russian SolarWinds Attackers Launch New Wave of Cyber Espionage Attacks

Source: https://www.cysecurity.news/2023/04/russian-solarwinds-attackers-launch-new.html

From the Article: "Russian intelligence has once more employed hacker outfit Nobelium/APT29 as part of its ongoing invasion of Ukraine, this time to spy on foreign ministries and diplomats from NATO-member states as well as additional targets in the European Union and Africa. "

Additional Sources:
https://www.darkreading.com/vulnerabilities-threats/russian-intel-services-behind-barrage-espionage-cyberattacks

FROZENBARENTS group targets energy sector, as Ukraine remains Russia’s biggest cyber focus this year - Industrial Cyber

Source: https://industrialcyber.co/threat-landscape/frozenbarents-group-targets-energy-sector-as-ukraine-remains-russias-biggest-cyber-focus-this-year/

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

From the Article: "Google's Threat Analysis Group (TAG) identified in a report this week that it continues to disrupt campaigns from multiple Russian government-backed attackers who are focused on the war in Ukraine in the first quarter of this year. The Google report also threw light on the FROZENBARENTS aka Sandworm group, attributed to Russian Armed Forces' Main Directorate of the General Staff (GRU) Unit 74455 which targets the energy sector and continues to hack and leak operations. "

Additional Sources:
https://industrialcyber.co/threat-landscape/frozenbarents-group-targets-energy-sector-as-ukraine-remains-russias-biggest-cyber-focus-this-year/

US Medical Service Data Breach Impacts 2.3M People

Source: https://heimdalsecurity.com/blog/us-medical-service-data-breach-impacts-2-3m-people/

From the Article: "Shields Health Care Group (SHCG), a medical service provider in the United States, announced a data breach that compromised the personal information of more than 2.3 million people."

Additional Sources:
https://www.darkreading.com/attacks-breaches/shields-health-breach-exposes-2-3m-users-data

ChatGPT Can be Tricked To Write Malware When You Act as a Developer Mode

Source: https://gbhackers.com/chatgpt-can-be-tricked-to-write-malware/

From the Article: "Japanese cybersecurity experts warn that ChatGPT can be deceived by users who input a prompt to mimic developer mode, leading the AI chatbot to generate code for malicious software. Developers' security measures to deter unethical and criminal exploitation of the tool have been exposed as easily bypassed by this revelation."

Additional Sources:
https://www.cysecurity.news/2023/04/chatgpt-researcher-develops-malicious.html

Infoblox Uncovers DNS Malware Toolkit & Urges Companies to Block Malicious Domains

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

Source: https://www.darkreading.com/vulnerabilities-threats/infoblox-uncovers-dns-malware-toolkit-urges-companies-to-block-malicious-domains

From the Article: "Infoblox Inc. the company that delivers a simplified, cloud- enabled networking and security platform for improved performance and protection, today published a threat report blog on a remote access trojan (RAT) toolkit with DNS command and control (C2)."

Additional Sources:
https://www.cysecurity.news/2023/04/dns-malware-toolkit-discovered-by.html

Hackers are Employing This Top Remote Access Tool to Get Unauthorised Access to Your Company's Networks

Source: https://www.cysecurity.news/2023/04/hackers-are-employing-this-top-remote.html

From the Article: "Another genuine enterprise software platform is being misused by cybercriminals to deliver malware and ransomware to unwitting victims. The DFIR Report's cybersecurity analysts identified many threat actors using Action1 RMM, an otherwise benign remote desktop monitoring and management tool."

Additional Sources:
https://www.cysecurity.news/2023/04/hackers-exploit-action1-rmm-in.html

Mandiant 2023 M-Trends Report Provides Factual Analysis of Emerging Threat Trends

Source: https://www.securityweek.com/mandiant-2023-m-trends-report-provides-factual-analysis-of-emerging-threat-trends/

From the Article: "In a year dominated by kinetic/cyber war in Ukraine, North Korea doubles down on cryptocurrency thefts, China and Iran continue to take advantage, and a new form of personal intimidation of company personnel emerges."

Additional Sources:
https://www.csoonline.com/article/3693575/businesses-detect-cyberattacks-faster-despite-increasingly-sophisticated-adversaries.html

Sotero Introduces Ransomware Protection Technology - PR Newswire

Link back to Table of Contents

The articles have been 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.prnewswire.com/news-releases/sotero-introduces-ransomware-protection-technology-301800516.html

From the Article: " In advance of RSAC 2023, Sotero, the leader in revolutionary data security, today announced the availability of Sotero Ransomware Protection, giving organizations the ability to proactively protect unstructured data from attack by utilizing behavior-based detection."

Additional Sources:
https://www.helpnetsecurity.com/2023/04/21/sotero-ransomware-protection/

China's Guangdong Plans $4.4bn Fund to Boost Chip Sector

Source: https://www.asiafinancial.com/chinas-guangdong-plans-4-4bn-fund-to-boost-chip-sector

From the Article: "Yuecai Holdings announced the fund, which will have a 17-year term and invest in auto chips and equipment for microchips, at an event on Tuesday, the Securities Times said"

Additional Sources:
https://www.scmp.com/tech/big-tech/article/3217482/tech-war-chinas-guangdong-province-doubles-down-semiconductor-expansion-40-new-projects-worth-us74

FERC authorizes incentive rate treatment for cybersecurity investments - Industrial Cyber

Source: https://industrialcyber.co/utilities-energy-power-water-waste/ferc-authorizes-incentive-rate-treatment-for-cybersecurity-investments/

From the Article: "The Federal Energy Regulatory Commission (FERC) issued Thursday a final rule providing incentive-based rate treatment for utilities making certain voluntary cybersecurity investments. The rule follows Congress' direction under the Infrastructure Investment and Jobs Act (IIJA) of 2021 that the Commission revise its regulations to establish incentive-based rate treatments to encourage utilities to invest in advanced cybersecurity technology and participate in cybersecurity threat information sharing programs for the benefit of consumers. "

Additional Sources: https://www.ferc.gov/news-events/news/ferc-approves-incentive-rate-treatment-cybersecurity-investments

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

Two new chipmaking industry clusters taking shape in Japan

Source: https://www.digitimes.com/news/a20230418PD207/euv-ic-manufacturing-japan-must-read-semiconductor.html

From the Article: "Japan is attempting to revitalize its chipmaking sector and strengthen related industry supply chains. Its current focus is on logic ICs. As a result of this strategy, two new chipmaking industry clusters in Japan will be taking shape: one in Kumamoto..."

Additional Sources:
https://www.digitimes.com/news/a20230417PD202/chiplet-chips+components-ic-manufacturing-japan.html

Samsung sees 12-inch fab capacity utilization rise to 90% on stable 5/4nm process yields

Source: https://www.digitimes.com/news/a20230418PD203/12-inch-fab-capacity-ic-manufacturing-samsung-electronics.html

From the Article: "Samsung Electronics has seen its 12-inch wafer fab capacity utilization rise to 90% in the second quarter from 80% registered a quarter earlier, driven by stable 5/4nm process performance and the resulting increase in customer orders, according to Korean..."

Additional Sources: https://www.digitimes.com/news/a20230417PD203/samsung-mpw-semiconductor-foundry.html

Russian APT Hackers Increasingly Attacking NATO Allies in Europe

Source: https://www.cysecurity.news/2023/04/russian-apt-hackers-increasingly.html

From the Article: "In accordance with the Polish CERT and Military Counterintelligence Service, an ongoing cyberespionage effort linked to a Russian nation-state entity is targeting European government agencies and diplomats in order to collect Western government intelligence on the Ukraine war."

Additional Sources:
https://www.rand.org/blog/2023/04/countering-russias-nuclear-threat-in-europe.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.

Triple Extortion and Erased Data are the New Ransomware Norm - Security Intelligence

Source: https://securityintelligence.com/articles/triple-extortion-erased-data-new-ransomware-norm/

From the Article: "The old days of “honest” ransomware gangs are long gone. In the past, ransomware groups pressured each other to honor file decryption promises after the ransom was paid. However, their motives were far from altruistic. They thought victims would be less willing to pay if word got out that their files would never be recovered. Today, the game has changed dramatically."

Additional Sources:
https://securityboulevard.com/2023/04/threat-spotlight-triple-extortion-ransomware/

2023 Phishing Report Reveals 47.2% Surge in Phishing Attacks Last Year

Source: https://www.zscaler.com/blogs/security-research/2023-phishing-report-reveals-472-surge-phishing-attacks-last-year

From the Article: "Phishing attacks continue to be one of the most significant threats facing organizations today. As businesses increasingly rely on digital communication channels, cybercriminals exploit vulnerabilities in email, SMS, and voice communications to launch sophisticated phishing attacks. With the COVID-19 pandemic leading to a surge in remote work over the past several years, the risk of phishing attacks has only increased."

Additional Sources:
https://informationsecuritybuzz.com/phishing-operations-escalating-threat-actors-utilize-ai-tools/

Misconfiguration leaves thousands of servers vulnerable to attack, researchers find

Source: https://cyberscoop.com/misconfiguration-servers-vulnerable-censys/

From the Article: "The firm that indexes internet-facing devices found that more than 8,000 servers hosting sensitive information such as log-in credentials, database backups and configuration files are not property configured."

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

Additional Sources: https://www.csoonline.com/article/3693260/weak-credentials-unpatched-vulnerabilities-malicious-oss-packages-causing-cloud-security-risks.html

This New Cybercrime Group Uses Ransomware to Target Businesses

Source: https://www.cysecurity.news/2023/04/this-new-cybercrime-group-uses.html

From the Article: "Researchers in cybersecurity have detailed the techniques of a "rising" cybercriminal group known as "Read The Manual" (RTM) Locker, which operates as a private ransomware-as-a-service (RaaS) provider and conducts opportunistic attacks to make illegal profit."

Additional Sources: https://www.oodaloop.com/briefs/2023/04/19/rtm-locker-gang-targets-corporate-environments-with-ransomware/

European Commission adopts proposal for EU Cyber Solidarity Act to strengthen cybersecurity capacities

Source: https://industrialcyber.co/regulation-standards-and-compliance/european-commission-adopts-proposal-for-eu-cyber-solidarity-act-to-strengthen-cybersecurity-capacities/

From the Article: "The European Commission adopted Tuesday a proposal for the EU Cyber Solidarity Act to strengthen cybersecurity capacities in the region. It will support the detection and awareness of cybersecurity threats and incidents, and bolster the preparedness of critical entities, apart from reinforcing solidarity, concerted crisis management, and response capabilities across Member States."

Additional Sources:
https://www.welivesecurity.com/2023/04/19/eu-cyber-solidarity-act-security-operations-centers-rescue/

EFF on the UN Cybercrime Treaty

Source: https://www.schneier.com/blog/archives/2023/04/eff-on-the-un-cybercrime-treaty.html

From the Article: "EFF has a good explainer on the problems with the new UN Cybercrime Treaty, currently being negotiated in Vienna."

Link back to Table of Contents

The articles have been 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://thecyberwire.com/newsletters/policy-briefing/5/76

TSMC's Heroic Assumption – Low Utilization Rates, Fab Cancellation, 3nm Volumes, Automotive Weakness, AI Advanced Packaging Demands, 2024 Capex Weakness

Source: https://www.semianalysis.com/p/tsmcs-heroic-assumption-low-utilization

From the Article: "Can these heroic assumptions be supported? Tremendous risk."

Additional Sources:
https://www.digitimes.com/news/a20230421PD200/apple-ic-manufacturing-iphone-tsmc.html

DHS Announces AI Task Force, Security Sprint On China Related Threats

Source: https://www.scmagazine.com/news/strategy/dhs-announces-ai-task-force-security-sprint-on-china-related-threats

From the Article: "The Department of Homeland Security announced a pair of initiatives that will directly feed into the United States' strategies for defending critical infrastructure and essential services from cyber attacks, physical attacks, artificial intelligence and other threats.

Additional Sources:
https://cyberscoop.com/mayorkas-china-sprint-ai-task-force/

2023 Thales Data Threat Report reveals alarming increase in ransomware attacks and ...

Source: https://techobserver.in/2023/04/19/2023-thales-data-threat-report-reveals-alarming-increase-in-ransomware-attacks-and-cloud-data-breaches/

From the Article: "Thales has released the 2023 Thales Data Threat Report, an annual report that surveys nearly 3000 IT and security professionals in 18 countries to identify the latest data security threats, trends, and emerging topics. According to this year's report, there has been an

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.crn.in/news/increase-in-ransomware-attacks-and-human-error-as-main-cause-of-cloud-data-breaches-globally-thales-data-threat-report/

The Good, the Bad and the Ugly in Cybersecurity - Week 16 - SentinelOne

Source: https://www.sentinelone.com/blog/the-good-the-bad-and-the-ugly-in-cybersecurity-week-16-4/

From the Article: "Two Chrome zero-days urgently patched, LockBit ransomware takes a swipe at macOS, and Linux malware tied to 3CX attack."

Fake Chrome updates spread malware

Source: https://www.malwarebytes.com/blog/news/2023/04/fake-chrome-updates-spread-malware

From the Article: "Compromised websites are causing big headaches for Chrome users. A campaign running since November 2022 is using hacked sites to push fake web browser updates to potential victims."

Cyber Security Today, April 21, 2023 – Is the LockBit ransomware gang slipping, or is IT ...

Source: https://www.itworldcanada.com/article/cyber-security-today-april-21-2023-is-the-lockbit-ransomware-gang-slipping-or-is-it-allowing-them-to-look-good/537332

From the Article: "Welcome to Cyber Security Today. It's Friday, April 21st, 2023. I'm Howard Solomon, contributing reporter on cybersecurity for ITWorldCanada.com and TechNewsday.com in the U.S."

LockBit Ransomware Reportedly Strikes Venezuela's Largest Bank - BeInCrypto

Source: https://beincrypto.com/lockbit-ransomware-attack-strikes-venezuelas-largest-bank/

From the Article: "Twitter users are reporting that Banco de Venezuela, the largest bank in the country, has fallen victim to a ransomware attack. Cybersecurity portals monitoring these attacks have confirmed the information."

Link back to Table of Contents

An Analysis of the BabLock (aka Rorschach) Ransomware

Source: https://www.trendmicro.com/en_us/research/23/d/an-analysis-of-the-bablock-ransomware.html

Summary: TrendMicro analysis of the BabLock ransomware. Overview of the common packages used in the ransomware to encrypt, the file extensions applied to impacted files, and common indicators of compromise.

Gary Bowser, Former Nintendo Hacker, Released From Prison

Source: https://www.darkreading.com/endpoint/gary-bowser-former-nintendo-hacker-released-from-prison

From the Article: "Originally sentenced to 40 months in prison, the former Nintendo Switch hacker is being released early due to good behavior but still owes millions."

17th April – Threat Intelligence Report

Source: https://research.checkpoint.com/2023/17th-april-threat-intelligence-report/

From the Article: "Two major automotive manufacturers Hyundai and Toyota have disclosed significant data breaches. Hyundai's Italian and French car owners were affected, along with individuals who booked a test drive. The leaked data consists of clients' personal information including emails, addresses, phone numbers, and vehicle chassis numbers. "

Xage's multi-layer access management solution bolsters cybersecurity of OT, ICS environments

Source: https://industrialcyber.co/vendor/xages-multi-layer-access-management-solution-bolsters-cybersecurity-of-ot-ics-environments/

From the Article: "Zero trust security firm Xage announced its multi-layer access management solution, which provides a defense-in-depth approach to every asset across operational technology (OT) and industrial control system (ICS) environments."

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

New infosec products of the week: April 21, 2023 - Help Net Security

Source: https://www.helpnetsecurity.com/2023/04/21/new-infosec-products-of-the-week-april-21-2023/

From the Article: "Here's a look at the most interesting products from the past week, featuring releases from Armorblox, Cofense, D3 Security, Sotero, Venafi, Veracode, Versa Networks, and Zyxel Networks."

Veracode Fix helps organizations tackle software security issues

Source: https://www.helpnetsecurity.com/2023/04/19/veracode-fix/

From the Article: "Veracode launches Veracode Fix, a new AI-powered product that suggests remediations for security flaws found in code and open-source dependencies. Shifting the paradigm from merely 'find' to 'find and fix' "For far too long, organizations have had to choose between remediating software security flaws and meeting aggressive deadlines to push code into production."

Dragos OT-CERT bolsters industrial environments, supply chains with cybersecurity resources for SMBs

Source: https://industrialcyber.co/vendor/dragos-ot-cert-bolsters-industrial-environments-supply-chains-with-cybersecurity-resources-for-smbs/

From the Article: "It has been a year since industrial cybersecurity company Dragos launched its OT-CERT (Operational Technology – Cyber Emergency Readiness Team) cybersecurity resource program, designed to provide industrial asset owners and operators with free OT-specific cybersecurity resources to help them build their OT cybersecurity programs, improve their security postures, and reduce OT risk."

Fortinet Training Institute's 2023 ATC Award Winners are Helping to Close the Cyber Skills Gap

Source: https://www.fortinet.com/blog/business-and-technology/fortinet-atc-award-winners-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: "Read more about Fortinet's 2023 ATC Awards that recognize exceptional achievements in quality of training delivery, customer experience, and more."

Orange Cyberdefense strengthens position in healthcare security sector

Source: https://www.helpnetsecurity.com/2023/04/21/orange-cyberdefense-healthcare-sector/

From the Article: "Orange Cyberdefense has been selected to carry out cyber crisis management exercises by the GIP SESAN (Groupement Régional d'Appui au Développement de l'eSanté d'Île-de-France) and by CAIH (Centrale d'Achat de l'Informatique Hospitalière) to support healthcare players in the region."

Weekly Cyber Threat Report, April 10 – 14, 2023

Source: https://cyberintelmag.com/threat-intelligence/weekly-cyber-threat-report-april-10-14-2023/

From the Article: "This week's good news includes CISA ordering government entities to upgrade their Macs and iPhones by May 1st, Adobe addressing security vulnerabilities in Reader and Acrobat, Fortinet fixing a severe flaw in a data analytics solution, WhatsApp coming up with a new device feature to prevent account takeover attacks, and much more."

[Arm and a Leg] Cyber Insurers Are Worried About The Long-tail Cost of Attacks

Source: https://blog.knowbe4.com/arm-and-a-leg-cyber-insurers-are-worried-about-the-long-tail-cost-of-attacks

From the Article: "James Rundle at the The Wall Street Journal today published a very interesting article about the long-term costs of cyber attacks and the fact that cyber insurers are getting more and more worried that their models do not cover these long-tail repercussions."

Two-step supply-chain attack. Plugging leaks, in both Mother Russia and the Land of the Free and the Home of the Brave. Belarus remains a player in the cyber war.

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

Source: https://thecyberwire.com/podcasts/daily-podcast/1806/notes

From the Article: "The 3CX compromise involved a two-stage supply-chain attack. Impersonating ChatGPT. Russia's security organs say they're cracking down on leaks. Updates on the Discord Papers case. "

Iranian threat actor exploits N-day vulnerabilities. US Air Force opens investigation into alleged leaker's ANG wing. Russia-Ukraine disinformation update.

Source: https://thecyberwire.com/newsletters/week-that-was/7/16

From the Article: "Iranian threat actor exploits N-day vulnerabilities. US Air Force opens investigation into alleged leaker's ANG wing. 3CX compromise involved a two-stage supply-chain attack."

Lazarus Group's Deathnote Cluster: A Threat to the Defense Sector

Source: https://www.cysecurity.news/2023/04/lazarus-groups-deathnote-cluster-threat.html

From the Article: "The Lazarus Group, a well-known cybercriminal organization, has pivoted to the defense sector with its Deathnote cluster. The group has previously been linked to cryptocurrency attacks and other malicious activities. However, its latest move into the defense industry marks a significant shift in its operations."

Experts Warn Patching Won't Protect Critical Infrastructure Against New Age Malware

Source: https://www.scmagazine.com/analysis/security-awareness/experts-warn-patching-wont-protect-critical-infrastructure-against-new-age-malware

From the Article: "The world’s most advanced industrial malware, PIPEDREAM, could be hiding within critical infrastructure control systems ready to unleash its “wartime capabilities,” a management consultancy has warned."

EvilExtractor malware activity spikes in Europe and the U.S. - Bleeping Computer

Source: https://www.bleepingcomputer.com/news/security/evilextractor-malware-

Link back to Table of Contents

activity-spikes-in-europe-and-the-us/

From the Article: "Researchers are seeing a rise in attacks spreading the EvilExtractor data theft tool, used to steal users' sensitive data in Europe and the U.S."

How to Spot and Avoid Phishing Scams While Gambling Online

Source: https://www.itsecurityguru.org/2023/04/19/how-to-spot-and-avoid-phishing-scams-while-gambling-online/

From the Article: "Online casinos and other gambling websites have revolutionized how many gamblers play. Whereas gambling used to be restricted to specific physical locations, punters can now freely enjoy a quick betting session regardless of where they are. "

The continuing threat of ransomware: some trends.

Source: https://thecyberwire.com

From the Article: "Two recent studies highlight the continuing threat of ransomware."

APT43: An investigation into the North Korean group's cybercrime operations

Source: https://blog.virustotal.com/2023/04/apt43-investigation-into-north-korean.html

From the Article: "As recently reported by our Mandiant's colleagues, APT43 is a threat actor believed to be associated with North Korea. APT43's main targets include governmental institutions, research groups, think tanks, business services, and the manufacturing sector, with most victims located in the United States and South Korea."

The role of ai in pcb manufacturing and assembly

Source: https://electronics360.globalspec.com/article/19472/the-role-of-ai-in-pcb-manufacturing-and-assembly

From the Article: "Due to disruptions caused by the COVID-19 pandemic and geopolitical tensions, there are major weak spots in the supply chain to which printed

circuit board (PCB) manufacturers and the businesses and governments that depend on them are vulnerable. The development of everything from autos to medical gadgets and key infrastructure has been hampered by the well-documented global scarcity of semiconductors, PCBs and other essential electronic components."

PCBAA Reacts to Implications of Biden's PCB Determination

Source: http://pcb.iconnect007.com/index.php/article/135841/pcbaa-reacts-to-implications-of-bidens-pcb-determination/135844/?skin=pcb

From the Article: "Hot on the heels of the news that U.S. President Biden signed a presidential determination in support of the printed circuit board industry, I-Connect007's Nolan Johnson spoke with David Schild, executive director of the Printed Circuit Board Association of America, about some of the expected implications. David points out, among other things, that this signals increased momentum with government and defense to support U.S.-based printed circuit manufacturing, and the possibility that a renewed interest in the industry by private financing could possibly follow. "

Sensor market set to bounce back in second half of 2023; Japanese corporations ready to go

Source: https://www.digitimes.com/news/a20230419PD204/chips+components-japan-passive-pcb-other-ic-components-sensor.html

From the Article: "Japan has estimated that the global sensor market in fiscal year 2022 (2022/04–2023/03) will decline as it was affected by the semiconductor market downturn that began in 2022, and the situation in the first half of fiscal year 2023 is not looking..."

Will 2023 Be an Inflection Point for CFIUS?

Source: https://www.nationaldefensemagazine.org/articles/2023/4/7/will-2023-be-an-inflection-point-for-cfius

From the Article: "...2023 is looking like a pivotal moment for national security regulation, with the Committee on Foreign Investment in the United States, or CFIUS, and a potential outbound screening regime at the center of attention."

Link back to Table of Contents

Battery Bird protects customers from vulnerabilities in public Wifi networks

Source: https://www.helpnetsecurity.com/2023/04/18/battery-bird-charging-kiosk/

From the Article: "Recent warnings by the FBI and FCC have highlighted the risks associated with using public USB chargers. Hackers have created ways to use public USB ports to introduce malware and monitoring software onto the phones of unsuspecting users."

Anomali Cyber Watch: Cozy Bear Employs New Downloaders, RTM Locker Ransomware Seeks Privacy, Vice Society Automated Selective Exfiltration

Source: https://www.anomali.com/blog/anomali-cyber-watch-cozy-bear-employs-new-downloaders-rtm-locker-ransomware-seeks-privacy-vice-society-automated-selective-exfiltration

From the Article: "The various threat intelligence stories in this iteration of the Anomali Cyber Watch discuss the following topics: APT, Clicker, Conversation hijacking, Data exfiltration, Malspam, Phishing, Ransomware, Russia, and Supply chain."

CommScope compromised by Vice Society ransomware, data leaked | SC Media

Source: https://www.scmagazine.com/brief/uncategorized/commscope-compromised-by-vice-society-ransomware-data-leaked

From the Article: "Individuals in Australia and Poland have been subjected to attacks with the novel Android banking trojan dubbed 'Chameleon,' since January, with the malware impersonating the cryptocurrency exchange CoinSpot, an Australian government agency, and Poland's IKO bank, according to BleepingComputer."

Threat Source newsletter (April 20, 2023) — Preview of Cisco and Talos at RSA

Source: https://blog.talosintelligence.com/threat-source-newsletter-april-20-2023-preview-of-cisco-and-talos-at-rsa/

From the Article: "We're firing up the conference circuit again for 2023, kicking things off next week with the RSA Conference in San Francisco. Cisco has a ton of exciting announcements, keynotes and talks lined up for the week, but there are also plenty of Talos-focused events to take in."

Link back to Table of Contents

Play ransomware's new tools. A look at what the GRU's been up to. US Air Force opens investigation into alleged leaker's Air National Guard wing. KillNet's new hacker course: "Dark School."

Source: https://thecyberwire.com/podcasts/daily-podcast/1805/notes

From the Article: "Play ransomware's new tools. Fancy Bear is out and about. Updates on Sandworm. Ransomware in Russia's war against Ukraine. The US Air Force opens an investigation into the alleged leaker's Air National Guard wing. The Washington Post's Tim Starks joins us with insights on the Biden administration's attempts to better secure the water supply."

5 Cybersecurity Pillars Where 85% of Companies Are Lagging

Source: https://www.bankinfosecurity.com/blogs/5-cybersecurity-pillars-where-85-companies-are-lagging-p-3437

From the Article: "Cisco's Cybersecurity Readiness Index shows a mere 15% of global organizations rank as mature across five security pillars."

New ransomware groups target VMWare and Linux | Kaspersky official blog

Source: https://www.kaspersky.com/blog/linux-vmware-esxi-ransomware-attacks/47988/

From the Article: "Ransomware. Nasty. But how to build defenses against it? Rather – what should be protected first and foremost? Often, Windows workstations, Active Directory servers, and other Microsoft products are the prime candidates. And this approach is usually justified. But we should bear in mind that cybercriminal tactics are constantly evolving, and malicious tools are now being developed for Linux servers and virtualization systems. In 2022, the total number of attacks on Linux systems increased by about 75%."

Week in review: 5 free online cybersecurity resources for SMBs, AI tools might fuel BEC attacks

Source: https://www.helpnetsecurity.com/2023/04/23/week-in-review-5-free-online-

Link back to Table of Contents

cybersecurity-resources-for-smbs-ai-tools-might-fuel-bec-attacks/

From the Article: "In this Help Net Security interview, Alicja Cade, Director, Financial Services, Office of the CISO, Google Cloud, offers insights on how asking the right questions can help improve cyber performance and readiness, advance responsible AI practices, and balance the need for cybersecurity with other business priorities."

Breach Roundup: US CFPB, NCR and Rheinmetall - BankInfoSecurity

Source: https://www.bankinfosecurity.com/breach-roundup-us-cfpb-ncr-rheinmetall-a-21727

From the Article: "Every week, Information Security Media Group rounds up cybersecurity incidents and breaches around the world. In the days between April 14 and April 20, the spotlight was on the U.S. Consumer Financial Protection Bureau, a ransomware attack on American payments firm NCR, German automotive and arms producer Rheinmetall, State agencies in the Philippines, and popular Indian rental platform RentoMojo."

CVE-2023-2246

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-2246

From the Article: "A vulnerability has been found in SourceCodester Online Pizza Ordering System 1.0 and classified as critical. This vulnerability affects unknown code of the file admin/ajax.php?action=save_settings. "

CVE-2023-23753

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-23753

From the Article: "The 'Visforms Base Package for Joomla 3' extension is vulnerable to SQL Injection as concatenation is used to construct an SQL Query. An attacker can interact with the database and could be able to read, modify and delete data on it."

CVE-2022-45074

Link back to Table of Contents

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-45074

From the Article: "Cross-Site Request Forgery (CSRF) vulnerability in Paramveer Singh for Arete IT Private Limited Activity Reactions For Buddypress plugin <=Â 1.0.22 versions."

CVE-2022-45080

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-45080

From the Article: "Cross-Site Request Forgery (CSRF) vulnerability in KrishaWeb Add Multiple Marker plugin <=Â 1.2 versions."

CVE-2023-23816

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-23816

From the Article: "Auth. (admin+) Cross-Site Scripting (XSS) vulnerability in Twardes Sitemap Index plugin <=Â 1.2.3 versions."

CVE-2023-23817

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-23817

From the Article: "Auth. (contrinbutor+) Cross-Site Scripting (XSS) vulnerability in WebArea | Vera Nedvyzhenko Simple PDF Viewer plugin <=Â 1.9 versions."

CVE-2023-22718

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-22718

From the Article: "Reflected Cross-Site Scripting (XSS) vulnerability in Jason Lau User Meta Manager plugin <=Â 3.4.9 versions."

CVE-2023-24386

Link back to Table of Contents

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-24386

From the Article: "Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Karishma Arora AI Contact Us Form plugin <=Â 1.0 versions."

CVE-2022-4944

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-4944

From the Article: "A vulnerability, which was classified as problematic, has been found in kalcaddle KodExplorer up to 4.49. Affected by this issue is some unknown functionality. The manipulation leads to cross-site request forgery."

CVE-2023-2243

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-2243

From the Article: "A vulnerability was found in SourceCodester Complaint Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file users/registration.php of the component POST Parameter Handler. The manipulation of the argument fullname leads to sql injection. "

CVE-2023-2244

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-2244

From the Article: "A vulnerability was found in SourceCodester Online Eyewear Shop 1.0. It has been classified as critical. This affects an unknown part of the file /admin/orders/update_status.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection."

CVE-2023-2245

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-2245

From the Article: "A vulnerability was found in hansunCMS 1.4.3. It has been declared

as critical. This vulnerability affects unknown code of the file /ueditor/net/controller.ashx?action=catchimage. "

CVE-2023-2241

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-2241

From the Article: "A vulnerability, which was classified as critical, was found in PoDoFo 0.10.0. Affected is the function readXRefStreamEntry of the file PdfXRefStreamParserObject.cpp. The manipulation leads to heap-based buffer overflow. An attack has to be approached locally. The exploit has been disclosed to the public and may be used."

CVE-2023-2242

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-2242

From the Article: "A vulnerability has been found in SourceCodester Online Computer and Laptop Store 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the component GET Parameter Handler. The manipulation of the argument c/s leads to sql injection."

CVE-2023-25506

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-25506

From the Article: "NVIDIA DGX-1 contains a vulnerability in Ofbd in AMI SBIOS, where a preconditioned heap can allow a user with elevated privileges to cause an access beyond the end of a buffer, which may lead to code execution, escalation of privileges, denial of service and information disclosure."

Microsoft shifts to a new threat actor naming taxonomy

Source: https://www.microsoft.com/en-us/security/blog/2023/04/18/microsoft-shifts-to-a-new-threat-actor-naming-taxonomy/

From the Article: "Today, Microsoft is excited to announce that we are shifting to a new

threat actor naming taxonomy aligned to the theme of weather. The complexity, scale, and volume of threats is increasing, driving the need to reimagine not only how Microsoft talks about threats but also how we enable customers to understand those threats quickly and with clarity."

IMDRF guidance covers principles and practices for cybersecurity of legacy medical devices

Source: https://industrialcyber.co/medical/imdrf-guidance-covers-principles-and-practices-for-cybersecurity-of-legacy-medical-devices/

From the Article: "The International Medical Device Regulators Forum (IMDRF) published last week a document that sets forth foundational security principles and best practices that span the total product life cycle (TPLC) of medical devices. Global adoption of the guidance is predicated on consistent implementation of the recommendations contained within it."

Zelle users targeted with social engineering tricks

Source: https://www.helpnetsecurity.com/2023/04/14/zelle-social-engineering/

From the Article: "Cybercriminals have been leveraging social engineering techniques to impersonate the popular US-based digital payments network Zelle and steal money from unsuspecting victims, according to Avanan."

Living Off the Land (LOTL) attacks: Detecting ransomware gangs hiding in plain sight

Source: https://www.malwarebytes.com/blog/business/2023/04/living-off-the-land-lotl-attacks-detecting-ransomware-gangs-hiding-in-plain-sight

From the Article: "Regular readers of our monthly ransomware review (read our April edition here) know that Ransomware-as-a-Service (RaaS) gangs have been making headlines globally with their disruptive attacks on organizations."

Joruri Gw vulnerable to cross-site scripting

Source: https://jvn.jp/en/jp/JVN87559956/

Link back to Table of Contents

From the Article: "Joruri Gw provided by SiteBridge Inc. contains a cross-site scripting vulnerability."

7 cybersecurity mindsets that undermine practitioners and how to avoid them

Source: https://www.csoonline.com/article/3693255/7-cybersecurity-mindsets-that-undermine-practitioners-and-how-to-avoid-them.html

From the Article: "It's no secret that cybersecurity jobs are burning people out. It's a high-pressure environment that ever seems to be ratcheting up the daily demand on security professionals."

7 tips for tackling cyber security technical debt

Source: https://www.cybertalk.org/2023/04/17/7-tips-for-tackling-cyber-security-technical-debt/

From the Article: "The cyber risk landscape is evolving. Novel attack types are appearing at an unprecedented rate. Cyber criminals are constantly seeking new ways to infiltrate networks, paralyze systems, steal data and drive their own financial gains."

How machine learning algorithms detect ransomware attacks

Source: https://www.cybertalk.org/2023/04/12/how-machine-learning-algorithms-detect-ransomware-attacks/

From the Article: "How can businesses and users stay ahead of the ever-evolving risk of ransomware attacks? An increasing number of cyber attacks occur every year, posing a serious threat to users' privacy and financial well-being. Fortunately, machine learning can give users an edge over hackers using pattern recognition and behavioral analysis."

New landscapes in cloud security (2023)

Source: https://www.cybertalk.org/2023/04/14/new-landscapes-in-cloud-security-2023/

From the Article: "In this outstanding CyberTalk interview, cloud security expert Richard

Flanders shares perspectives surrounding the latest cloud security architecture trends and challenges."

Xiaoqiying/Genesis Day Threat Actor Group Targets South Korea, Taiwan

Source: https://www.recordedfuture.com/xiaoqiying-genesis-day-threat-actor-group-targets-south-korea-taiwan

From the Article: "Xiaoqiying (aka Genesis Day, Teng Snake) is a primarily Chinese-speaking threat group that is most well known for conducting website defacement and data exfiltration attacks on more than a dozen South Korean research and academic institutions in late-January 2023."

Top 7 Attack Surface Metrics You Should Keep Track Of

Source: https://www.recordedfuture.com/popular-attack-surface-metrics

From the Article: "Organizations are constantly sprinting to manage and control their scattered workforces and growing attack surfaces. Unfortunately, this is a situation that cybercriminals have been quick to take advantage of; the trend toward complexity and increased interconnectedness of digital systems has brought an increase in potential entry points for malicious actors seeking unauthorized access to networks and systems."

2023 Ransomware Attacks: First-Quarter Highlights

Source: https://www.reliaquest.com/blog/2023-ransomware-attacks-q1/

From the Article: "The post 2023 Ransomware Attacks: First-Quarter Highlights appeared first on ReliaQuest."

Naivas admits to data theft, attack contained - The Star

Source: https://www.the-star.co.ke/news/realtime/2023-04-23-naivas-admits-to-data-theft-attack-contained/

From the Article: "In a statement, Naivas said it has contained the attack, and systems

are secure, adding that operations are normal. "

Decoy Dog malware toolkit found after analyzing 70 billion DNS queries

Source: https://www.bleepingcomputer.com/news/security/decoy-dog-malware-toolkit-found-after-analyzing-70-billion-dns-queries/

From the Article: "A new enterprise-targeting malware toolkit called 'Decoy Dog' has been discovered after inspecting anomalous DNS traffic that is distinctive from regular internet activity."

What to Expect From Ransomware Gang Attacks in 2023 - ReadWrite

Source: https://readwrite.com/what-to-expect-from-ransomware-gang-attacks/

From the Article: "Criminals profit from ransomware. It pays off and works, just like all malware on the Internet of Things. In the previous year, phishing or ransomware is the subject of a recent Trend Micro survey."

6 Mac antivirus options to improve internet security | TechTarget

Source: https://www.techtarget.com/searchenterprisedesktop/tip/Mac-antivirus-options-to-improve-internet-security

From the Article: "Organizations that support macOS desktops need to protect them with antivirus software that safeguards against the many lurking threats to business systems and data."

More malware, less ransomware in higher ed

Source: https://www.insidehighered.com/news/tech-innovation/administrative-tech/2023/04/21/more-malware-less-ransomware-higher-ed

From the Article: "Cybercriminals are humans, and as such, their whims, preferences and practices are subject to change. In 2020 and 2021, across sectors and regions, they appeared to prefer ransomware over other kinds of malware attacks, and government was their top malware target, according to new report from SonicWall."

Link back to Table of Contents

Investors Bet Big on Safe Security for Cyber Risk Management

Source: https://www.securityweek.com/investors-bet-big-on-safe-security-for-cyber-risk-management/

From the Article: "Safe Security, a startup building technology to help organizations manage cyber risk, has secured a $50 million Series B funding round."

What's next for crypto

Source: https://www.technologyreview.com/2022/12/20/1064940/whats-next-for-crypto-2023/

From the Article: "The battle lines are complicated, but there are two prominent sides. A vocal crowd of crypto skeptics, which includes prominent politicians and regulators, wants to rein in an industry it sees as overrun with fraud and harmful to consumers. The catastrophic demise of FTX has emboldened this group."

Cyber Security Today, April 19, 2023 – Ransomware gang hits CommScope, unsanitized ...

Source: https://www.itworldcanada.com/article/cyber-security-today-april-19-2023-ransomware-gang-hits-commscope-unsanitized-routers-being-re-sold-and-more/536768

From the Article: "Welcome to Cyber Security Today. It's Wednesday, April 19th, 2023. I'm Howard Solomon, contributing reporter on cybersecurity for ITWorldCanada.com and TechNewsday.com in the U.S."

Tabs Manager Pro adware

Source: https://www.2-spyware.com/remove-tabs-manager-pro-adware.html

From the Article: "Tabs Manager Pro is a browser extension that acts as adware and shows pop-up ads Tabs Manager Pro is marketed as a tool for managing browser tabs, but it is actually adware."

Link back to Table of Contents

American Bar Association (ABA) suffered a data breach,1.4 million members impacted

Source: https://securityaffairs.com/145125/data-breach/american-bar-association-data-breach.html

From the Article: "The American Bar Association (ABA) disclosed a data breach, threat actors gained access to older credentials for 1,466,000 members."

Challenges facing China's development of AI chatbots

Source: https://www.digitimes.com/news/a20230421PD207/ai-china-internet-security-must-read.html

From the Article: "Since Baidu pioneered China's homegrown development of ChatGPT-like AI chatbots with its Ernie Bot, several businesses have followed suit, including SenseTime's SenseNova and Alibaba Cloud's Tongyi Qianwen. Huawei also intends to release an upgraded..."

Hikvision optimistic about market recovery; expands investment in automotive and AI products

Source: https://www.digitimes.com/news/a20230421PD203/china-hikvision-surveillance-video-camera.html

From the Article: "China-based video surveillance equipment maker Hikvision released its 2022 financial report. It reported a revenue of CNY83.2 billion (US$12.08 billion), a 2.1% annual growth. In terms of the net profit attributed to the parent company, it reached CNY12.8..."

Hikvision Denies Leaked Pentagon Spy Claim

Source: https://www.bbc.com/news/world-asia-china-65307503

From the Article: "It was responding to BBC queries about allegations revealed in a recently leaked Pentagon document."

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

Lilac-Reloaded For Nagios 2.0.8 Remote Code Execution

Source: https://packetstormsecurity.com/files/171940/lrn208-exec.txt

From the Article: "Lilac-Reloaded for Nagios version 2.0.l8 remote code execution exploit."

FUXA 1.1.13-1186 Remote Code Execution

Source: https://packetstormsecurity.com/files/171956/fuxa11131186-exec.txt

From the Article: "FUXA version 1.1.13-1186 suffers from an unauthenticated remote code execution vulnerability."

Lawsuit tries to hold Apple responsible for fake apps

Source: https://www.securingindustry.com/lawsuit-tries-to-hold-apple-responsible-for-fake-apps/s112/a15220/

From the Article: "Baidu has filed lawsuits against various software developers that it says have violated intellectual property it holds on its Ernie Bot app, an artificial intelligence-powered chatbot that aims to rival OpenAI's ChatGPT and Google's Bard."

RichExts browser hijacker

Source: https://www.2-spyware.com/remove-richexts-browser-hijacker.html

From the Article: "RichExts is a hijacker that changes the main browser settings and raises security concerns RichExts is a browser hijacker that can cause a variety of undesirable symptoms."

Lacework adds vulnerability risk management to its flagship offering

Source: https://www.csoonline.com/article/3693990/lacework-adds-vulnerability-risk-managemenlaceworks-risk-based-vulnerabit-to-its-flagship-offering.html

From the Article: "The SaaS capability will combine active package detection, attack

path analysis, and in-house data on active exploits to generate personalized vulnerability risk scores."

App cyberattacks jump 137%, with healthcare, manufacturing hit hard, Akamai says

Source: https://www.csoonline.com/article/3693712/app-cyberattacks-jump-137-with-healthcare-manufacturing-hit-hard-akamai-says.html

From the Article: "An analysis of customer data collected by content delivery network and internet services giant Akamai found that attacks targeting web applications rose by 137% over the course of last year, as the healthcare and manufacturing sectors in particular were targeted with an array of API and application-based intrusions."

Iranian threat actor exploits N-day vulnerabilities. Subdomain hijacking vulnerabilities. The Discord Papers. An update on Russia's NTC Vulkan. And weather reports, not a Periodic Table.

Source: https://thecyberwire.com/podcasts/daily-podcast/1804/notes

From the Article: "An Iranian threat actor exploits N-day vulnerabilities. CSC exposes subdomain hijacking vulnerabilities. More on the Discord Papers. An update on Russia's NTC Vulkan."

Microsoft Will Name Threat Actors After Weather Events

Source: https://www.securityweek.com/microsoft-will-name-apts-actors-after-weather-events/

From the Article: "Microsoft plans to use weather-themed naming of APT actors as part of a move to simplify the way threat actors are documented."

You think patching Windows is a pain? Try patching a Mars rover millions of miles away - ZDNet

Source: https://www.zdnet.com/article/you-think-patching-windows-is-a-pain-try-patching-a-mars-rover-142-million-miles-away/

Link back to Table of Contents

Summary: Mars rover Curiosity was patched with a significant update. The update had been in the works since 2016 and was about 22 MB, it took several days to transmit the data from Earth to Mars and a couple of days to apply the patch to the rover.

10th April – Threat Intelligence Report

Source: https://research.checkpoint.com/2023/10th-april-threat-intelligence-report/

From the Article: "A ransomware attack has affected New Jersey Camden County's police department. According to reports, while the attack has been going on since the middle of March, the department has not yet managed to repair its systems. Meanwhile, criminal investigation files have been locked and are inaccessible."

DOJ accuses China of using 'police station' in Manhattan to spy on dissidents inside US

Source: https://abc7ny.com/china-spy-nyc-police-station/13143281/

From the Article: "NEW YORK (WABC) -- The FBI on Monday revealed what it said is evidence of expanding espionage and security activity by the Chinese government on U.S. soil, including in Lower Manhattan. The Justice Department announced three cases suggesting more brazen activity by China inside the U.S. in the wake of the spy balloon controversy. One case involves Chinese security officials allegedly spying on Zoom calls and then harassing Chinese dissident participants identified as targets."

CrowdStrike Announces Managed XDR to Close the Cybersecurity Skills Gap, Expands MDR Portfolio

Source: https://www.darkreading.com/endpoint/crowdstrike-announces-managed-xdr-to-close-the-cybersecurity-skills-gap-expands-industry-leading-mdr-portfolio

From the Article: "CrowdStrike (Nasdaq: CRWD) today introduced CrowdStrike Falcon Complete XDR, a new Managed eXtended Detection and Response (MXDR) service from the MDR and endpoint security market leader. CrowdStrike Falcon Complete XDR extends the elite expertise of its industry-leading MDR service, which includes 24/7 expert management, threat hunting, monitoring and end-to-end remediation, across all key attack surfaces to close the cybersecurity skills gap."

Link back to Table of Contents

Quantifying cyber risk vital for business survival

Source: https://www.helpnetsecurity.com/2023/04/19/cyber-attacks-financial-impact/

From the Article: "Healthcare, manufacturing, and utilities are suffering long-term financial impact of major cyber attacks, according to ThreatConnect. “With the National Cyber Strategy coming out of the White House focusing on decreasing cyber risk from critical infrastructure and the new SEC Cyber Proposals, organizations across industries are now being tasked with reporting on cyber risk,” said Jerry Caponera, GM of Risk Quantification, ThreatConnect."

Cyberattacks Can Cost Enterprises Up to 30% of Operating Income According to ThreatConnect

Source: https://www.darkreading.com/attacks-breaches/cyber-attacks-can-cost-enterprises-up-to-30-percent-of-operating-income-according-to-new-research-from-threatconnect

From the Article: "Risk quantification research finds healthcare, manufacturing, and utilities suffer long-term financial impact from major cyberattacks."

[webapps] ProjeQtOr Project Management System 10.3.2 - Remote Code Execution (RCE)

Source: https://www.exploit-db.com/exploits/51387

From the Article: "ProjeQtOr Project Management System 10.3.2 - Remote Code Execution (RCE)."

MacStealer – newly-discovered malware steals passwords and exfiltrates data from infected Macs

Source: https://grahamcluley.com/macstealer-newly-discovered-malware-steals-passwords-and-exfiltrates-data-from-infected-macs/

From the Article: "I'm still encountering people who, even after all these years, believe that their Apple Mac computers are somehow magically invulnerable to ever being infected by malware."

Link back to Table of Contents

Preventing Malware & Cyber Attacks: Simple Tips for Your Computer

Source: https://www.hackread.com/preventing-malware-cyber-attacks-on-computer/

From the Article: "Living without the Internet is hardly imaginable today. However, the anonymity of the internet has led to the flourishing of cyber attacks and malware. Malicious software can cause damage to our devices, steal personal data, and lead to monetary loss. Therefore, protecting your computer from these threats is crucial. This article will outline some methods and resources for protecting your devices from malicious software, and explain why it's essential to use malware removal at all times."

Forecast: demand for picking robots to jump by 2030

Source: https://www.dcvelocity.com/articles/57162-forecast-demand-for-picking-robots-to-jump-by-2030

From the Article: "Rising labor costs and dropping robot prices will boost installations, Interact Analysis says."

Small Business is a Big Priority: NIST Expands Outreach to the Small Business Community

Source: https://www.nist.gov/blogs/cybersecurity-insights/small-business-big-priority-nist-expands-outreach-small-business

From the Article: "On March 6, 2023, NIST launched a new small business initiative that will create more opportunities for the exchange of information, resources, and ideas between NIST and the nation's small business community via the creation of a new Small Business Community of Interest. The COI will bring together the small business community, companies, trade associations, and others who can share business insights, expertise, challenges, and perspectives to guide our work."

Why xIoT Devices Are Cyberattackers' Gateway Drug for Lateral Movement

Source: https://www.darkreading.com/ics-ot/why-xiot-devices-are-gateway-drug-lateral-movement

From the Article: "Detailing how extended IoT (xIoT) devices can be used at scale by attackers to establish persistence across networks and what enterprises should start

doing about the risk."

Western Digital Hack – Attackers Demanding "Minimum 8 Figures" as Ransom

Source: https://gbhackers.com/western-digital-cyber-attack/

From the Article: "WD (Western Digital), the data storage solutions provider, recently announced a distressing announcement. In a cybersecurity incident, their network suffered a data breach that allowed threat actors to unauthorizedly access data across multiple systems."

QuaDream says goodnight. Data breach at US bank. Can ChatGPT replace the psychologist's couch?

Source: https://thecyberwire.com/newsletters/privacy-briefing/5/76

From the Article: "QuaDream says goodnight. Data breach at US bank. Can ChatGPT replace the psychologist's couch? New England healthcare organization investigates cyber incident."

Critical Flaws in vm2 JavaScript Library Can Lead to Remote Code Execution

Source: https://thehackernews.com/2023/04/critical-flaws-in-vm2-javascript.html

From the Article: "A fresh round of patches has been made available for the vm2 JavaScript library to address two critical flaws that could be exploited to break out of the sandbox protections."

Military helicopter crash blamed on failure to apply software patch

Source:
https://www.theregister.com/2023/04/18/helicopter_crash_missing_software_patch/

From the Article: "An Australian military helicopter crash was reportedly caused by failure to apply a software patch, with a hefty side serving of pilot error."

Link back to Table of Contents

Medusa ransomware crew brags about spreading Bing, Cortana source code

Source: https://www.theregister.com/2023/04/19/medusa_microsoft_data_dump/

From the Article: "The Medusa ransomware gang has put online what it claims is a massive leak of internal Microsoft materials, including Bing and Cortana source code."

5 Types of Cyber Crime Groups

Source: https://www.trendmicro.com/en_us/ciso/22/k/cyber-crime-group-types.html

From the Article: "Discover the five main types of cyber crime groups: access as a service, ransomware as a service, bulletproof hosting, crowd sourcing, and phishing as a service as well as tips to strengthen your defense strategy."

Pakistani Hackers Use Linux Malware Poseidon to Target Indian Government Agencies

Source: https://thehackernews.com/2023/04/pakistani-hackers-use-linux-malware.html

From the Article: "The Pakistan-based advanced persistent threat (APT) actor known as Transparent Tribe used a two-factor authentication (2FA) tool used by Indian government agencies as a ruse to deliver a new Linux backdoor called Poseidon."

Cybersecurity M&A Roundup for April 1-15, 2023

Source: https://www.securityweek.com/cybersecurity-ma-roundup-for-april-1-15-2023/

From the Article: "Sixteen cybersecurity-related M&A deals were announced in the first half of April 2023."

2023 Vulnerabilities: First-Quarter Highlights

Source: https://www.reliaquest.com/blog/2023-q1-vulnerabilities-cves/

From the Article: "The post 2023 Vulnerabilities: First-Quarter Highlights appeared first on ReliaQuest."

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

March 2023 broke ransomware attack records with 459 incidents - Bleeping Computer

Source: https://www.bleepingcomputer.com/news/security/march-2023-broke-ransomware-attack-records-with-459-incidents/

From the Article: "March 2023 was the most prolific month recorded by cybersecurity analysts in recent years, measuring 459 attacks, an increase of 91% from the previous month and 62% compared to March 2022."

Scary ransomware group Royal is on the rise - Business Plus

Source: https://businessplus.ie/industry-type/technology/scary-ransomware/

From the Article: "New ransomware group Royal has launched numerous attacks in recent months, according to NordLocker, the file security tool for individuals and businesses."

Stephen Starr Gift Card Sales Stopped By Ransomware Attack - Philadelphia Magazine

Source: https://www.phillymag.com/news/2023/04/20/stephen-starr-gift-cards-ransomware/

From the Article: "Want to buy a gift card to Parc? Buddakan? El Vez? Perhaps Le Coucou in New York City? You can't. These are all Stephen Starr restaurants, and a major ransomware attack has suspended gift card sales at all of them for more than a week."

This New Mirai Variant Uses Peculiar Malware Distribution Methods

Source: https://www.cysecurity.news/2023/04/this-new-mirai-variant-uses-peculiar.html

From the Article: "RapperBot, a new Mirai variant, is the latest example of malware spreading through relatively uncommon or previously undiscovered infection channels. RapperBot originally appeared last year as Internet of Things (IoT) malware that contained big amounts of Mirai source code but had significantly different capabilities than other Mirai variants."

Link back to Table of Contents

Spyware Offered to Cyberattackers via PyPI Python Repository

Source: https://www.cysecurity.news/2023/04/spyware-offered-to-cyberattackers-via.html

From the Article: "The attackers, who Sonatype researchers linked to the SylexSquad malware-as-a-service (MaaS) gang in Spain, gave their programme a not-so-subtle name: "reverse-shell." Reverse shells are programmes that are often used by hackers to run commands remotely and receive data from targeted machines."

Security Issues in FINS protocol

Source: https://jvn.jp/en/ta/JVNTA91513661/

From the Article: "FINS (Factory Interface Network Service) is a message communication protocol, which is designed to be used in closed FA (Factory Automation) networks, and is used in FA networks composed of Omron products. Recent security researches show multiple issues against systems speaking FINS protocol."

Friendly Hacker, Keren Elazari, to Announced as Keynote Speaker at Infosecurity Europe 2023

Source: https://www.infosecurity-magazine.com/news/karen-elazari-infosecurity-europe/

From the Article: "Acclaimed analyst and author, Keren Elazari, to deliver keynote exploring the intersection of cyber conflict and politics at Infosecurity Europe 2023."

Tight budgets and burnout push enterprises to outsource cybersecurity

Source: https://www.helpnetsecurity.com/2023/04/19/cybersecurity-professionals-responsibilities/

From the Article: "With cybersecurity teams struggling to manage the remediation process and monitor for vulnerabilities, organizations are at a higher risk for security breaches, according to Cobalt."

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

Edgio Advanced Bot Management protects users against bot attacks

Source: https://www.helpnetsecurity.com/2023/04/19/edgio-advanced-bot-management/

From the Article: "Edgio has released Advanced Bot Management solution that proactively mitigates a wide range of evolving malicious bots while providing observability into good bots."

5 free online cybersecurity resources for small businesses

Source: https://www.helpnetsecurity.com/2023/04/19/small-business-free-cybersecurity/

From the Article: "As cyberattacks increase in frequency and sophistication, small and medium-sized businesses (SMBs) become more vulnerable to cyber threats. Unlike larger enterprises, SMBs often lack the financial and technical resources to secure their networks and data against malicious actors effectively."

Cofense Protect+ defends mid-size organizations from cyber threats

Source: https://www.helpnetsecurity.com/2023/04/21/cofense-protect/

From the Article: "Cofense has released Cofense Protect+, a fully integrated and automated email security solution specifically designed to protect mid-size organizations from ever-evolving cyber threats."

CISA warns of OS Command Injection vulnerability in INEA ME RTU hardware - Industrial Cyber

Source: https://industrialcyber.co/cisa/cisa-warns-of-os-command-injection-vulnerability-in-inea-me-rtu-hardware/

From the Article: "The U.S. Cybersecurity and Infrastructure Security Agency (CISA) published Thursday a security advisory rated as CVSS 10.0 severity, identifying the presence of an OS Command Injection vulnerability in INEA ME RTU (Remote Terminal Unit) equipment. The RTU works as a data interface between the remote device and the control center"

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

Increased globalized exposure to ransomware attacks will continue to define ICS cyber threat landscape

Source: https://industrialcyber.co/features/increased-globalized-exposure-to-ransomware-attacks-will-continue-to-define-ics-cyber-threat-landscape/

From the Article: "Ransomware attacks on critical infrastructure have been rapidly increasing and pose a greater threat to operational technology (OT) assets and control systems. In recent years, the quantity and range of ransomware infections targeting industrial organizations have significantly increased, exemplified by cases, such as EKANS and the Colonial Pipeline attacks."

Terravision - 2,075,625 breached accounts

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

From the Article: "In February 2023, the European airport transfers service Terravision suffered a data breach. The breach exposed over 2M records of customer data including names, phone numbers, email addresses, salted password hashes and in some cases, date of birth and country of origin."

38 Countries Take Part in NATO's 2023 Locked Shields Cyber Exercise

Source: https://www.securityweek.com/38-countries-take-part-in-natos-2023-locked-shields-cyber-exercise/

Summary: Initial summary of the 2023 NATO Locked Shields exercise

CISA: Why Healthcare Is No Longer Off-Limits for Attackers

Source: https://www.bankinfosecurity.com/interviews/healthcare-no-longer-off-bounds-for-attackers-i-5243

From the Article: "Healthcare entities of all types and sizes could be the next targets of major cybersecurity attacks, said Nitin Natarajan, deputy director of the Cybersecurity and Infrastructure Security Agency."

Link back to Table of Contents

Why Lifescience Industry is witnessing rising Cyberattacks - ET HealthWorld

Source: https://health.economictimes.indiatimes.com/news/health-it/why-lifescience-industry-is-witnessing-rising-cyberattacks/99679482

From the Article: "Cyber security has become very critical in every sector as cyber-attacks have been on the rise. Ransomware attacks are becoming increasingly common and involve hackers gaining control of a victim's systems and demanding payment in exchange for restoring access to their data."

Ransomware attacks hit an all-time in March 2023 - gHacks Tech News

Source: https://www.ghacks.net/2023/04/22/ransomware-attacks-record-march/

From the Article: "The record-breaking ransomware attack activity in March 2023 serves as a reminder of the critical need for robust cybersecurity measures."

Software-Dependency Data Delivers Security to Developers

Source: https://www.darkreading.com/dr-tech/software-dependency-data-delivers-security-to-developers

From the Article: "Google has opened up its software-dependency database, adding to the security data available to developers and tool makers. Now developers need to use it."

Military Tech Execs Tell Congress an AI Pause Is 'Close to Impossible'

Source: https://gizmodo.com/ai-chatgpt-military-congress-hearing-pause-impossible-1850354878

From the Article: "Tech execs used a congressional hearing to scold the Pentagon for its sluggish AI development and encourage more spending on tech to "terrify adversaries.""

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

How to Build AI-Powered Cybersecurity Applications

Source: https://www.sans.org/blog/how-to-build-ai-powered-cybersecurity-applications/

From the Article: "In the era of rapidly advancing technology, the security community is constantly seeking new and innovative ways to safeguard their organizations. The recent WebCast session, Beyond ChatGPT, Building Security Applications using OpenAI API, emphasized the need to shift focus from only using ChatGPT to building security applications with AI models."

System-level testing demand rising; TSMC, Intel, and other foundries are in

Source: https://www.digitimes.com/news/a20230418PD205/ic-manufacturing-must-read-probe-card-semiconductor-industry-testing.html

From the Article: "System-level testing demand for advanced ICs has been rising. Foundries including TSMC, Intel and Samsung Electronics, as well as OSATs such as ASE Technology, are already involved, according to industry sources."

Intel CPUs vulnerable to new transient execution side-channel attack

Source: https://www.bleepingcomputer.com/news/security/intel-cpus-vulnerable-to-new-transient-execution-side-channel-attack/

Summary: New side channel attack leverages a flaw in transient execution that can exfiltrate secrets based on a timing attack.

GlobalFoundries sues IBM, says trade secrets were unlawfully given to Japan's Rapidus

Source: https://www.reuters.com/technology/globalfoundries-sues-ibm-says-trade-secrets-were-unlawfully-given-japans-rapidus-2023-04-19/

From the Article: "New York-based GlobalFoundries said in its complaint that IBM had shared IP and trade secrets with Rapidus, a new state-backed Japanese consortium that IBM is working with to develop and produce cutting-edge two-nanometre chips. It also asserted that IBM had unlawfully disclosed and misused its IP with Intel Corp (INTC.O), noting that IBM had announced in 2021 it would collaborate with Intel on next-generation chip 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.

GlobalFoundries, RPI partner on semiconductor manufacturing course

Source: https://www.timesunion.com/business/article/globalfoundries-rpi-partner-semiconductor-17904228.php

From the Article: "Class has 70 students, which is double a typical upper-level elective at RPI"

A Brief History of the MOS transistor, Part 4: IBM Research, Persistence, and the Technology No One Wanted

Source: https://www.eejournal.com/article/a-brief-history-of-the-mos-transistor-part-4-ibm-research-persistence-and-the-technology-no-one-wanted/

From the Article: "Furthermore, no new commercial machines or devices shall be announced which make primary use of tube circuitry." That policy would put IBM into the transistor business – the bipolar transistor business."

Micron nsf join 21 top universities semi network

Source: https://www.fierceelectronics.com/embedded/micron-nsf-join-21-top-universities-semi-network

From the Article: "Micron and the National Science Foundation have formed an unusual partnership with 21 prestigious universities in the Northeast and Mid-Atlantic to support workforce development efforts laid out in the CHIPS and Science Act."

Machine Learning and Semiconductor Manufacturing

Source: https://www.azom.com/article.aspx?ArticleID=22592

From the Article: "This article discusses the relationship between machine learning (ML) and semiconductor manufacturing, specifically the application of ML algorithms and models in the semiconductor manufacturing process."

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

3 semiconductor plants announced for Jalisco and Baja California

Source: https://mexiconewsdaily.com/business/3-semiconductor-plants-announced-for-jalisco-and-baja-california/

From the Article: "Three technology companies will establish electronic semiconductor chip manufacturing plants in Jalisco and Baja California to meet worldwide demand, according to the head of the National Auto Parts Industry (INA) business chamber, Alberto Bustamante."

Process Innovation Unveiled for Through-Glass Vias in Advanced Packaging and Display Applications

Source: https://displaydaily.com/process-innovation-unveiled-for-through-glass-vias-in-advanced-packaging-and-display-applications/

From the Article: "In a collaborative effort, Germany's Plan Optik and 4JET have developed a cutting-edge process chain for the high-speed production of metallized through-glass vias (TGV) using what they call volume laser induced structuring (VLIS) technology. "

Why Your Anti-Fraud, Identity & Cybersecurity Efforts Should Be Merged

Source: https://www.darkreading.com/vulnerabilities-threats/why-your-anti-fraud-identity-cybersecurity-efforts-should-be-merged

From the Article: "To address the rising risk of online fraud, stolen identities, and cyberattacks, innovative organizations have begun converging their security functions — here's how yours can prepare."

Proactive Defense: Using Deception Against Ransomware Attacks

Source: https://www.fortinet.com/blog/industry-trends/offensive-defense-using-deception-against-ransomware-attacks

From the Article: "Organizations around the world have been reporting on cyberattacks involving ransomware, and this is a trend that is expected to continue. Learn how to address ransomware attacks with deception."

Link back to Table of Contents

Ex-CEO of hacked therapy clinic sentenced for failing to protect patients' session notes

Source: https://www.bitdefender.com/blog/hotforsecurity/ex-ceo-of-hacked-therapy-clinic-sentenced-for-failing-to-protect-patients-session-notes/

From the Article: "A Finnish court has given the former CEO of a chain of psychotherapy clinics a suspended jail sentence after failing to adequately protect highly sensitive notes of patients' therapy sessions from falling into the hands of blackmailing hackers."

DoNot APT Hackers Attack Individuals Using Android Malware via Chatting Apps

Source: https://gbhackers.com/donot-apt-hackers-attack/

From the Article: "CYFIRMA recently detected a cyber-attack on a person living in Kashmir, India, and obtained two malware pieces from the victim's mobile download folder. The investigation of these samples links the recent cyber-attack to DoNot APT, which has a long-standing record of activity in the area."

Netwrix Annual Security Survey: 68% of Organizations Experienced a Cyberattack Within the Last 12 Months

Source: https://www.darkreading.com/attacks-breaches/netwrix-annual-security-survey-68-of-organizations-experienced-a-cyberattack-within-the-last-12-months

From the Article: "The most common consequences were unplanned expenses, loss of competitive edge, and decreased sales."

3 Flaws, 1 War Dominated Cyber-Threat Landscape in 2022

Source: https://www.darkreading.com/ics-ot/three-flaws-one-war-dominated-cyber-threat-landscape-2022

From the Article: "Attackers continued to favor software exploits, phishing, and stolen credentials as initial-access methods last year, as Log4j and the Russia-Ukraine cyber conflict changed the threat landscape."

Link back to Table of Contents
The articles have been 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 structure of the global semiconductor market

Source: https://www.digitimes.com/news/a20230412VL206/ic-design-white-paper-ic-design-distribution-india-south-korea.html

From the Article: "DIGITIMES recently conducted a series of studies of the global IC design industry on behalf of TSIA."

India to counterbalance China

Source: https://www.digitimes.com/news/a20230418VL207/analysis-india.html&chid=10

From the Article: "Compared to other industry sectors, IC design has been more impacted by low birth rates and a lack of local IT manpower. In India, there are 56,000 IC design engineers; in the US, there are 86,000; in China, there are 121,000; and in Taiwan there are..."

India's auto sector demand alone could fill an entire foundry: industry insights

Source: https://www.digitimes.com/news/a20230418VL205/demand-foundry-ic-manufacturing-india.html

From the Article: "Even though there seems to be quite a delay in India's semiconductor manufacturing plans, local experts insist on its necessity for economic growth, technological development, and strategic autonomy. India is one of the largest consumers of semiconductors in the world, with applications ranging from smartphones and computers to automobiles and defense."

Apple commits to Make in India, reportedly to double employment there

Source: https://www.digitimes.com/news/a20230420VL200/apple-ict-manufacturing-india.html

From the Article: "Apple CEO Tim Cook made his first visit to India in seven years and met with Indian prime minister Narendra Modi as the world's largest company is looking to make India an iPhone production base."

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

WW Semiconductor Market Reached All-Time High in 2022

Source: https://www.storagenewsletter.com/2023/04/18/ww-semiconductor-market-reached-all-time-high-in-2022/

From the Article: "With revenue hitting $595.7 billion, DRAM and NAND and largerly beating NOR"

Farmers 'crippled' by satellite failure as GPS-guided tractors grind to a halt

Source: https://www.smh.com.au/national/farmers-crippled-by-satellite-failure-as-gps-guided-tractors-grind-to-a-halt-20230418-p5d1de.html

From the Article: "Tractors have ground to a halt in paddocks across Australia and New Zealand because of a signal failure in the satellite farmers use to guide their GPS-enabled machinery, stopping them from planting their winter crop."

Rheinmetall Suffers Another Cyberattack – Company Operations Still Functional

Source: https://heimdalsecurity.com/blog/rheinmetall-suffers-cyberattack/

From the Article: "Rheinmetall, a leading German armaments and technology company, was targeted by a cyberattack over the weekend. The attack, however, did not affect company operations, according to officials."

How companies are struggling to build and run effective cybersecurity programs

Source: https://www.helpnetsecurity.com/2023/04/20/build-run-effective-cybersecurity-programs-video/

From the Article: "A recent Code42 report reveals a rapidly growing number of inside risk incidents and a concerning lack of training and technology, further exacerbated by increasing workforce turnover and cloud adoption."

Outdated cybersecurity practices leave door open for criminals

Source: https://www.helpnetsecurity.com/2023/04/20/outdated-cybersecurity-practices/

Link back to Table of Contents
The articles have been 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: "Organizations experienced a significant increase in ransomware – from an average of four attacks over five years in 2021 versus four attacks over the course of one year in 2022, according to ExtraHop. Of those who fell victim, 83% admitted to paying the ransom at least once. "

Global EV Production: BYD Surpasses Tesla

Source: https://www.visualcapitalist.com/global-ev-production-byd-surpasses-tesla/

From the Article: "2022 was another historic year for EVs, with annual production surpassing 10 million cars for the first time ever. This represents a sizeable bump up from 2021's figure of 6.7 million. In this infographic, we've used data from EV Volumes to visualize the top 15 brands by output. The color of each brand's bubble represents their growth from 2021, with the darker shades depicting a larger percentage increase."

Cyber Threat Intelligence: The Power of Data

Source: https://www.trendmicro.com/en_us/ciso/23/d/cyber-threat-intelligence.html

From the Article: "Discover how cybersecurity leaders and decision makers can leverage cyber threat intelligence to increase security posture and reduce risk."

CISA Adds 3 Actively Exploited Flaws to KEV Catalog, including Critical PaperCut Bug

Source: https://thehackernews.com/2023/04/cisa-adds-3-actively-exploited-flaws-to.html

From the Article: "The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Friday added three security flaws to its Known Exploited Vulnerabilities (KEV) catalog, based on evidence of active exploitation."

European air traffic control confirms website 'under attack' by pro-Russia hackers

Source: https://www.theregister.com/2023/04/22/eurocontrol_russia_attack/

From the Article: "Europe's air-traffic agency appears to be the latest target in pro-Russian miscreants' attempts to disrupt air travel."

Link back to Table of Contents

Southwest Asks FAA to Issue Nationwide Ground Stop on its Flights

Source: https://jalopnik.com/southwest-asks-faa-issue-nationwide-ground-stop-flights-1850348051

Summary: Southwest Airlines asked for a nationwide ground stop on their air fleet due to an IT configuration issue.

Small Business Interest in Cyber-Hygiene is Waning

Source: https://www.infosecurity-magazine.com/news/small-business-interest-cyber/

From the Article: "UK government survey finds they are prioritizing other things."

Wargaming an effective data breach playbook

Source: https://www.helpnetsecurity.com/2023/04/18/effective-data-breach-playbook/

From the Article: "A well-tuned data breach playbook can provide security teams with a clear roadmap for working through the breach response process."

Stay Ahead of Cyberthreats with Proactive Threat Hunting

Source: https://heimdalsecurity.com/blog/proactive-threat-hunting/

From the Article: "In today's digital age, cyber threats are an ever-present danger to organizations of all sizes. From ransomware attacks to data breaches, the consequences of a successful cyberattack can be devastating."

Greenpeace says chip firms must cut emissions as electricity usage spikes

Source: https://www.scmp.com/business/article/3217640/greenpeace-says-chip-industry-electricity-consumption-more-double-2030-meaning-firms-must-cut

From the Article: "Greenpeace East Asia said it is now time for chip industry suppliers

Link back to Table of Contents

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

and component makers to step up to the plate on carbon emissions. Chip manufacturing is energy-intensive due to a long and complex production process, and currently relies heavily on fossil fuels."

Bitsight Expands into Integrated Cyber-Risk Management

Source: https://www.darkreading.com/risk/bitsight-expands-into-integrated-cyber-risk-management

From the Article: "Bitsight, a leader in managing and monitoring cyber risk, today unveiled its expansion into a broader category of integrated cyber risk management. As the category creator and global leader in the cybersecurity ratings industry, Bitsight's enhanced strategy will deliver new capabilities to empower security professionals and business leaders to more effectively and holistically manage cyber risk."

Latitude Financial Breaches Customer Data, Coles Warns

Source: https://www.cysecurity.news/2023/04/latitude-financial-breaches-customer.html

From the Article: "In an attempt to verify if the breach of Latitude Financial data was impacting Coles, the supermarket giant has confirmed it has. As part of the report, the company alleges that a cybercriminal gang has stolen the information used to issue previous Coles credit cards. "

Iranian threat actor exploits N-day vulnerabilities. Subdomain hijacking vulnerabilities. Discord Papers. Russia's NTC Vulkan.

Source: https://thecyberwire.com/newsletters/daily-briefing/12/74

From the Article: "Iranian threat actor exploits N-day vulnerabilities. Threat actor nomenclature. CSC exposes subdomain hijacking vulnerabilities. The Discord Papers. An update on Russia's NTC Vulkan."

Iranian threat actor exploits N-day vulnerabilities. US Air Force opens investigation into ...

Source: https://thecyberwire.com/newsletters/week-that-was/7/16

Link back to Table of Contents

From the Article: "Ransomware hits two-year high in March 2023. Russia-Ukraine disinformation update. Crime and punishment."

Iranian Hackers Using SimpleHelp Remote Support Software for Persistent Access

Source: https://thehackernews.com/2023/04/iranian-hackers-using-simplehelp-remote.html

From the Article: "The Iranian threat actor known as MuddyWater is continuing its time-tested tradition of relying on legitimate remote administration tools to commandeer targeted systems."

Takedown of GitHub Repositories Disrupts RedLine Malware Operations

Source: https://www.securityweek.com/takedown-of-github-repositories-disrupts-redline-malware-operations/

From the Article: "Four GitHub repositories used by RedLine stealer control panels were suspended, disrupting the malware's operations."

Blind Eagle Cyber Espionage Group Strikes Again: New Attack Chain Uncovered

Source: https://thehackernews.com/2023/04/blind-eagle-cyber-espionage-group.html

From the Article: "The cyber espionage actor tracked as Blind Eagle has been linked to a new multi-stage attack chain that leads to the deployment of the NjRAT remote access trojan on compromised systems."

Allies' plans for new AUKUS 'innovation initiatives' unveiled in DOD's 2024 budget request

Source: https://defensescoop.com/2023/04/17/allies-plans-for-new-aukus-innovation-initiatives-unveiled-in-dods-2024-budget-request/

From the Article: "A new cloud-based, international AI Development Hub is one of five projects planned."

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

Global semiconductor manufacturing equipment sales reach all-time record $108 billion

Source: https://roboticsandautomationnews.com/2023/04/18/global-semiconductor-manufacturing-equipment-sales-reach-all-time-record-108-billion/67347/

From the Article: "Worldwide sales of semiconductor manufacturing equipment increased 5 percent from $102.6 billion in 2021 to an all-time record of $107.6 billion last year, SEMI, the industry association representing the global electronics design and manufacturing supply chain."

KFC, Pizza Hut parent company suffers data breach after ransomware attack

Source: https://topclassactions.com/lawsuit-settlements/privacy/data-breach/kfc-pizza-hut-parent-company-suffers-data-breach-after-ransomware-attack/

From the Article: "Top Class Actions's website and social media posts use affiliate links. If you make a purchase using such links, we may receive a commission, but it will not result in any additional charges to you. Please review our Affiliate Link Disclosure for more information."

Vedanta signs MoUs with 20 Korean companies

Source: https://www.financialexpress.com/industry/vedanta-signs-mous-with-20-korean-companies/3051288/

From the Article: "Vedanta Group on Monday said it has signed MoUs with 20 Korean display glass companies for the development of an electronics manufacturing hub in India."

US tech firms should wargame response if China invades Taiwan, warns NSA cybersecurity chief

Source: https://breakingdefense.com/2023/04/us-tech-firms-should-wargame-response-if-china-invades-taiwan-warns-nsa-cybersecurity-chief/

From the Article: ""“You don't want to be starting that planning the week before an

invasion, when you're starting to see the White House saying it's coming," said NSA's Rob Joyce. "You want to be doing that now.""

Retail Giant Walmart Ranks First in List of Brands Most Likely to be Imitated in Phishing Attempts in Q1 2023

Source: https://blog.checkpoint.com/security/retail-giant-walmart-ranks-first-in-list-of-brands-most-likely-to-be-imitated-in-phishing-attempts-in-q1-2023/

From the Article: "Check Point Research's latest Brand Phishing Report reveals it is all change at the top for most imitated brands with new entries from financial services and retail Our latest Brand Phishing Report for Q1 2023 highlights the brands which were most frequently imitated by criminals in their attempts to steal individuals' personal information or payment credentials during January, February and March 2023."

Ransomware in Germany, April 2022 – March 2023

Source: https://www.malwarebytes.com/blog/threat-intelligence/2023/04/ransomware-review-germany

From the Article: "In August 2022, German power semiconductor manufacturer Semikron disclosed a ransomware attack that had partially encrypted its network, with the attackers claiming to have stolen 2TB of documents."

Firmware Caution Advises MSI Cyberattack

Source: https://www.cysecurity.news/2023/04/firmware-caution-advises-msi-cyberattack.html

From the Article: "Aside from gaming hardware manufacturers, modern corporations face constant attacks from malicious hackers and other digital no-goodniks. Corporations are not the only ones attacked by malicious hackers. MSI confirmed to its customers it had been attacked. "

Radware Bot Manager Protects Africa's Largest Drugstore and Grocery Chain From Damaging Bot Attacks

Link back to Table of Contents

Source: https://blog.radware.com/security/2023/04/radware-bot-manager-protects-large-africa-digital-strorefront/

From the Article: "A Radware Cloud Workload Protection client that is one of the largest drugstore and grocery chains in Africa turned to Radware's cybersecurity experts to help mitigate and prevent bot attacks that were executing account takeover (ATO) attacks on their customers' accounts."

API server of TONE Family vulnerable to authentication bypass using an alternate path

Source: https://jvn.jp/en/jp/JVN14492006/

From the Article: "API server of TONE Family provided by DREAM TRAIN INTERNET INC. contains an authentication bypass vulnerability using an alternate path."

PaperCut Warns of Exploited Vulnerability in Print Management Solutions

Source: https://www.securityweek.com/papercut-warns-of-exploited-vulnerability-in-print-management-solutions/

From the Article: "Print management solutions provider PaperCut warns that exploitation of a recently patched vulnerability has commenced."

A recession would solve 3 problems weighing on stocks: DataTrek

Source: https://markets.businessinsider.com/news/stocks/recession-outlook-stock-market-earnings-inflation-rates-labor-us-economy-2023-4

From the Article: "But markets have been buoyant in the face of those risks, DataTrek co-founder Nicholas Colas said, and a recession could remedy the "three most intractable problems" in markets that were spawned by the pandemic: 1) High inflation. Prices notched a 41-year-record in mid-2022, and still remain well-above the Fed's 2% inflation target – a factor that weighed heavily on corporate earnings and caused stocks to slump 20% in 2022. 2) Aggressive Fed rate hikes. Central bankers raised interest rates from historic lows over the last year to control inflation, which has squeezed firms with a higher borrowing costs and made bonds more attractive relative to equities. 3) Falling productivity in the labor market. The labor market has been incredibly robust in recent years, and a recession could stop companies from hoarding workers, which will improve profit margins."

Link back to Table of Contents

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

DOD Produces Climate Assessment Tool, Strengthens Climate Cooperation With Six Allies

Source: https://www.defense.gov/News/Releases/Release/Article/3369257/dod-produces-climate-assessment-tool-strengthens-climate-cooperation-with-six-a/

From the Article: "Over the past several months, department personnel have been engaged in tool development and climate change data identification with these allies, and today, the U.S. has delivered on that climate commitment. Sharing a customized version of DCAT with allies enhances their climate resilience, promotes security cooperation and interoperability and strengthens U.S. national security."

Securing the Future: The Next Wave of Cybersecurity

Source: https://casber.substack.com/p/securing-the-future-the-next-wave

From the Article: "Cybersecurity's Evolution & What's On the Horizon"

Va. launching semiconductor workforce initiative - Virginia Business

Source: https://www.virginiabusiness.com/article/va-launching-semiconductor-workforce-initiative/

From the Article: "The commonwealth is launching a Virginia Alliance for Semiconductor Technology to foster a semiconductor industry workforce, funding its establishment with a $3.3 million Growth and Opportunity for Virginia (GO Virginia) grant."

Sweden boosts national semiconductor industry with ClassIC program, backing European Chips Act - Innovation Origins

Source: https://innovationorigins.com/en/sweden-boosts-national-semiconductor-industry-with-classic-program-backing-european-chips-act/

From the Article: "DIGITAL - ClassIC unites key players for semiconductor collaboration, combating reliance on vulnerable supply chains in the sector"

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

Samsung hit with $303 million jury verdict in computer-memory patent lawsuit

Source: https://www.reuters.com/legal/samsung-hit-with-303-mln-jury-verdict-computer-memory-patent-lawsuit-2023-04-21/

From the Article: "April 21 (Reuters) - Computer-memory company Netlist Inc (NLST.PK) convinced a federal jury in Texas on Friday to award it more than $303 million for Samsung Electronics Co's (005930.KS) infringement of several patents related to improvements in data processing."

Semiconductors and Electrification Leading the Path to Sustainability

Source: https://www.analog.com/en/signals/articles/semiconductors-software-leading-path-to-sustainability.html

From the Article: "The semiconductor industry is on a major rebound growing at 26% year over year, now passing more than $600B of yearly revenue.2 That's nearly $100 per year for every person on Earth."

More engineers needed as semiconductor plants go up across Arizona

Source: https://www.abc15.com/news/state/more-engineers-needed-as-semiconductor-plants-go-up-across-arizona

From the Article: "As semiconductor factories go up across Arizona, there's a shortage of engineers qualified to do the job."

Who can damage, destroy in space? More than you think - 2023 report by Secure World Foundation

Source: https://www.linkedin.com/pulse/who-can-damage-destroy-space-more-than-you-think-2023-goward%3FtrackingId=uOshmDvO0NY3pXqKVbTMLA%253D%253D/?trackingId=uOshmDvO0NY3pXqKVbTMLA%3D%3D

From the Article: "Why its Important: The more we rely on space, the more attractive space assets become as targets for our adversaries. "

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

Ransomware: From the Boardroom to the Situation Room - BankInfoSecurity

Source: https://www.bankinfosecurity.com/ransomware-from-boardroom-to-situation-room-a-21732

From the Article: "She's been assistant general counsel at the CIA and undersecretary at the Department of Homeland Security. She is on the Cyberspace Solarium Commission. Now an adviser to the Center for Strategic and International Studies, Suzanne Spaulding will keynote at RSA Conference 2023."

Cyberspace Solarium Commission says space systems should be considered critical infrastructure

Source: https://cyberscoop.com/solarium-commission-space-systems-critical-infrastructure/

From the Article: "The Cyberspace Solarium Commission wants space systems to be considered critical infrastructure sector number 17, a move the influential group says will compel a growing industry of satellite operators to take action to better protect their networks from malicious hackers."

Mass Layoffs and Corporate Security Risks

Source: https://www.cysecurity.news/2023/04/mass-layoffs-and-corporate-security.html

From the Article: "Mass layoffs have become increasingly common in recent years as companies look to cut costs and remain competitive. While these layoffs can provide short-term financial benefits, they can also create new risks for corporate security."

Employing Zero Trust to Defend Against Backdoor Attacks

Source: https://www.cysecurity.news/2023/04/employing-zero-trust-to-defend-against.html

From the Article: "According to IBM's Security X-force Threat Intelligence Index 2023, hackers are prioritising these backdoor assaults in their efforts to blackmail downstream

Link back to Table of Contents

victims whose data has been hacked. The effort to breach a backdoor was the beginning of 21% of all intrusion attacks. A ransomware component was present in two-thirds of backdoor attempts."

Is Taiwan about to lose Paraguay, its last ally in South America?

Source: https://www.scmp.com/news/china/diplomacy/article/3217897/taiwan-about-lose-paraguay-its-last-ally-south-america

From the Article: "Polls have candidates neck-and-neck in presidential race, with the opposition's Efrain Alegre pledging to cut ties with Taipei. Whoever wins, there is growing pressure from Paraguay's largest economic sectors for a switch in diplomatic relations to Beijing."

EU takes on US and Asia with US$47 billion chip subsidy plan

Source: https://www.scmp.com/news/world/europe/article/3217509/eu-takes-us-and-asia-us47-billion-chip-subsidy-plan

From the Article: "The EU Chips Act aims to double the bloc's share of global semiconductor output to 20 per cent by 2030, and follows the US Chips for America Act. Asian companies, especially firms in China and Taiwan, currently dominate the manufacture and export of such chips."

Majority of Dutch companies are dissatisfied with own supply chain - Supply Chain Movement

Source: https://www.supplychainmovement.com/majority-of-dutch-companies-are-dissatisfied-with-own-supply-chain/

From the Article: "Almost all Dutch businesses are dissatisfied with their own supply chain, according to research by SAP. To improve this, most companies are looking for ways to make their supply chain more local. They also want to adopt new technology in the short term that will help them reduce risks and achieve greater sustainability."

Yes, AI is Using Brain Scans to Literally Read People's Minds - The Debrief

Link back to Table of Contents

Source: https://thedebrief.org/yes-ai-is-using-brain-scans-to-literally-read-peoples-minds/

From the Article: "A specially trained AI is using data collected from fMRI brain scans to read people's minds. And while the system must go through some initial training with the person whose thoughts it wants to read, the results are shockingly accurate, if not somewhat haunting."

Defense Official Confirms Leak: American Smart Bombs Are Failing in Ukraine - News From Antiwar.com

Source: https://news.antiwar.com/2023/04/16/defense-official-confirms-leak-american-smart-bombs-are-failing-in-ukraine/

From the Article: "Ukrainian forces' failure to correctly equip smart bombs and Russian jamming GPS signals are causing American-made weapons to miss their targets."

OTORIO-ServiceNow survey throws light on state of industrial OT cyber security, detects mindset shift - Industrial Cyber

Source: https://industrialcyber.co/analysis/otorio-servicenow-survey-throws-light-on-state-of-industrial-ot-cyber-security-detects-mindset-shift/

From the Article: "OTORIO, a manufacturer of OT cyber and digital risk management solutions, and ServiceNow announced survey results on Tuesday, revealing that OT has become a key component of critical infrastructure and industrial manufacturing, including power grids, transportation networks, and manufacturing facilities. The OTORIO-ServiceNow survey also identifies a definitive shift in OT cybersecurity strategy mindset from visibility (reactive approach) to risk management (preventative approach), indicating that 2023 and 2024 will be pivotal for operational security and critical infrastructure. "

The Tipping Point: Exploring the Surge in IoT Cyberattacks Globally

Source: https://blog.checkpoint.com/security/the-tipping-point-exploring-the-surge-in-iot-cyberattacks-plaguing-the-education-sector/

From the Article: "The first two months of 2023 have seen a 41% increase in the average number of weekly attacks per organization targeting IoT devices, compared to

2022. On average, every week 54% of organizations suffer from attempted cyber attacks targeting IoT devices IoT devices in European organizations are the most targeted, followed by those in APAC and Latin America-based organizations. "

Lawmakers Reintroduce Bill to Bolster Cybersecurity of K-12 Schools

Source: https://www.nextgov.com/cybersecurity/2023/04/lawmakers-reintroduce-bill-bolster-cybersecurity-k-12-schools/385366/

From the Article: "The bipartisan, bicameral legislation directs CISA to provide primary and secondary schools with more targeted cyber information and resources to combat a rise in ransomware attacks."

US bill to boost Taiwan cyberdefense - Taipei Times

Source: https://www.taipeitimes.com/News/front/archives/2023/04/22/2003798398

From the Article: "JOINT EXERCISES: A draft backed by four lawmakers from the House and Senate would authorize the Pentagon to work more closely with Taiwanese defense forces"

Italian group visited for chip talks, minister says - Taipei Times

Source: https://www.taipeitimes.com/News/taiwan/archives/2023/04/23/2003798458

From the Article: "KEY PARTNER: Italy has some strategic advantages in the chip industry, and trade with Taiwan is expected to increase this year, the representative office in Rome said"

Training on US weapons obligated by law: general - Taipei Times

Source: https://www.taipeitimes.com/News/front/archives/2023/04/22/2003798399

From the Article: "'KNIFE EDGE OF FREEDOM': Washington works with its allies in the first island chain to 'provide crisis response options,' US Army Japan Commanding General Joel Vowell said"

Link back to Table of Contents

AI Heightens Cyber Risk for Legacy Weapon Systems

Source: https://www.bankinfosecurity.com/generative-ai-heightens-cyber-risk-for-legacy-weapon-systems-a-21708

From the Article: "The U.S. weapons arsenal developed without a zero trust architecture is at growing risk from cyberattacks, lawmakers heard today in a panel dedicated to how artificial intelligence can simultaneously help and hurt efforts to protect warfighters from digital attacks."

TUSD provides update on ransomware attack investigation - KGUN 9

Source: https://www.kgun9.com/news/local-news/tusd-provides-update-on-ransomware-attack-investigation

From the Article: "The district has emphasized its commitment to transparency and the communication of accurate and verifiable information to its employees and families, especially in emergency situations."

Attackers extorting victims with fake ransomware claims - Technology Decisions

Source: https://www.technologydecisions.com.au/content/security/news/attackers-extorting-victims-with-fake-ransomware-claims-1055642631

From the Article: "Cybersecurity company Avast has uncovered evidence of a cybercrime group attempting to extort victims by sending emails attempting to trick customers into thinking they have fallen victim to a ransomware or data extortion attack."

Nanoimprint Finally Finds Its Footing

Source: https://semiengineering.com/nanoimprint-finds-its-footing-in-photonics/

From the Article: "Technology and business issues mean it won't replace EUV, but photonics, biotech and other markets provide plenty of room for growth."

Link back to Table of Contents

Oliver Dowden spells out Cyber 'Facts of Life' & announces New Alert to Belfast Conference!

Source: https://www.cybernewsgroup.co.uk/oliver-dowden-spells-out-cyber-facts-of-life-announces-new-alert-to-belfast-conference/

From the Article: "So it's great to complete the full Union set with Northern Ireland – & it's yet more proof that we have strong cyber talent in every corner of our country."

Russian Hacktivists Aspire to Attack Critical Infrastructure

Source: https://www.bankinfosecurity.com/russian-hacktivists-aspire-to-attack-critical-infrastructure-a-21706

From the Article: "Britain's National Cyber Security Centre said Russian hacktivists have ambitions of becoming a larger threat to Western critical infrastructure. "Disclosing this threat is not something we do lightly," said U.K. Cabinet Office Secretary of State Oliver Dowden."

Why cyber security should be treated as an ESG issue

Source: https://www.cybertalk.org/2023/04/20/why-cyber-security-should-be-treated-as-an-esg-issue/

From the Article: "The World Economic Forum describes cyber security as one of the top five global risks, highlighting the need for organizations to integrate cyber security into ESG risk management. As a result, effective oversight of security has become a priority for investors and regulators, who continue to push for robust oversight frameworks. "

March 2023's Most Wanted Malware: New Emotet Campaign Bypasses Microsoft Blocks to Distribute Malicious OneNote Files

Source: https://blog.checkpoint.com/security/march-2023s-most-wanted-malware-new-emotet-campaign-bypasses-microsoft-blocks-to-distribute-malicious-onenote-files/

From the Article: "Check Point Research reports that Emotet Trojan launched a new campaign last month to evade Microsoft's macro block, sending spam emails containing malicious OneNote files."

Link back to Table of Contents

The Power of Zero Trust in DevOps Supply Chains

Source: https://blog.checkpoint.com/securing-the-cloud/the-power-of-zero-trust-in-devops-supply-chains/

From the Article: "Building a DevOps supply chain requires thought and effort, and sometimes luck. Cyber security threats continue to increase as malicious actors become increasingly sophisticated, exposing businesses of all sizes. Today, it can be said with certainty that the only thing you can trust is distrust."

5 Ways to Improve Safety in The Construction Supply Chain

Source: https://www.allthingssupplychain.com/5-ways-to-improve-safety-in-the-construction-supply-chain/

From the Article: "Transportation and shipping jobs rank second on the list of positions with the most significant number of workplace injuries."

Maria Varmazis: Combining cyber and space. [Space]

Source: https://thecyberwire.com/podcasts/career-notes/146/notes

From the Article: "Maria Varmazis, N2K's Space Correspondent and host of N2K's newest podcast T-Minus, sits down to share her journey on combining her two passions of space and cyber."

How SMEs Can Secure the Remote Workforce - Infosecurity Magazine

Source: https://www.infosecurity-magazine.com/next-gen-infosec/sme-secure-remote-workforce/

From the Article: "As remote work becomes increasingly prevalent, small and medium-sized enterprises (SMEs) face a growing challenge of how to secure their remote workforce against cyber threats. With sensitive data and critical systems at risk, SMEs need to adopt best practices for 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.

Triple-digit Increase in API and App Attacks on Tech and Retail

Source: https://www.infosecurity-magazine.com/news/tripledigit-increase-api-app/

From the Article: "Web attacks also surge in financial services, although not in UK."

Why Cybercriminals Love The Rust Programming Language

Source: https://informationsecuritybuzz.com/cybercriminals-love-rust-programming/

From the Article: "The Rust programming language has been gaining popularity over the years due to its many advantages, including its high level of control, memory safety, and flexibility."

Building Equity in Cybersecurity Teams

Source: https://www.softsideofcyber.com/fostering-equity-in-cybersecurity-teams/

From the Article: "Equity in cybersecurity teams is vital for creating strong, resilient, and innovative defenses against cyber threats. Before we discuss how to promote equity, I want to explore the value we all get from it. This section will discuss the benefits of diversity and inclusion in these teams and explain how promoting equity can lead to higher employee satisfaction and retention."

Kimsuky: Infamous Threat Actor Churns Out More Advanced Malware

Source: https://www.zimperium.com/blog/kimsuky-infamous-threat-actor-churns-out-more-advanced-malware/

From the Article: "The Hacker News recently published a story that discusses a joint communication among the German intelligence apparatus, the Federal Office for the Protection of the Constitution (BfV), and South Korea's National Intelligence Service (NIS), warning readers about new tactics used by a North Korean threat actor called Kimsuky."

Link back to Table of Contents

South Korea's ICT export declined for nine consecutive months, with semiconductors dropping by 33.9%

Source: https://www.digitimes.com/news/a20230420PD204/ict-manufacturing-import_export-south-korea.html

From the Article: "Since the South Korean government started gathering import and export data on the ICT sector in 1996, the export value in March 2022 reached US$23.26 billion, a record high. However, fast forward to March 2023, ICT exports have declined for nine consecutive..."

Lam Research offers weak guidance for June quarter, optimistic about China market despite export ban

Source: https://www.digitimes.com/news/a20230420VL204/china-guidance-lam-research.html

From the Article: "Due to the downturn in the memory industry and the US export ban on semiconductor equipment against China, Lam Research provided weak guidance for the current quarter but expects less restrictive rules to export its products to China."

Recovery momentum still weak in China consumer electronics market, says GigaDevice

Source: https://www.digitimes.com/news/a20230420PD200/china-consumer-electronics-ic-design-distribution-mcu.html

From the Article: "China's consumer electronics market demand is not expected to recover significantly until the second half of the year despite a recent pick-up in retail sales, and the Double 11 shopping festival will be a critical indicator of the recovery momentum,..."

AMD joins AWS ISV Accelerate Program

Source: https://www.digitimes.com/news/a20230419PR201/amd-aws.html

From the Article: "AMD has announced it has joined the Amazon Web Services (AWS) Independent Software Vendor (ISV) Accelerate Program, a co-sell program for AWS Partners – like AMD – who provide integrated solutions on AWS. The program helps AWS Partners drive..."

Link back to Table of Contents

Xi's tech self-reliance push leaves Europeans wary of China R&D

Source: https://www.digitimes.com/news/a20230421VL211/china-r_d.html

From the Article: "China's push to become self-reliant in the technology sphere is driving more European companies operating there to rethink their research and development plans, according to a report published Friday by the European Union Chamber of Commerce in China..."

New IoT chip technologies gain attention; China turns to RISC-V for IoT chip development, says DIGITIMES Research

Source: https://www.digitimes.com/news/a20230421VL209/china-digitimes-research-risc-v-telecom-service-infrastructure.html

From the Article: "Broadband communication technologies such as LTE Cat.1bis and 5G NR-Light are gaining the attention of IoT chip developers for their new products with the phasing away of 2G and 3G networks, while IoT chips with RISC-V architecture have grown popular..."

Chinese attempt to 'leapfrog' in SiC/GaN not unchallenged

Source: https://www.digitimes.com/news/a20230421VL204/china-gan-sic.html

From the Article: "At the 2023 Optics Valley of China JFS Forum and Compound Semiconductor Industry Development Conference, Wu Lin, the President of China Advanced Semiconductor Industry Innovation Alliance, shared her observations on the current status of China's compound semiconductor development - a technology long deemed by the Chinese government as the country's chance to "leapfrog"."

Threat Report Reveals Hope Despite Active Threat Landscape

Source: https://www.bankinfosecurity.com/blogs/threat-report-reveals-hope-despite-active-threat-landscape-p-3433

From the Article: "Companies have rapidly adopted digital strategies to fuel growth and

profitability, yet many of these changes have inadvertently accelerated the risk of cyberattacks. As evidenced by the recently released 2023 OpenText Cybersecurity Threat Report, cybercriminals are taking advantage of these gaps."

eMemory security-enhanced OTP qualifies on TSMC N5

Source: https://www.digitimes.com/news/a20230419VL213/ememory-technology-heterogeneous-integration-ic-manufacturing-tsmc.html

From the Article: "NeoFuse, a security-enhanced version of eMemory's one-time programmable (OTP) non-volatile memory (NVM) technology, has been qualified on the TSMC N5 process. "

Hon Hai set to launch 5-10 qubit ion trap quantum computer within 5 years

Source: https://www.digitimes.com/news/a20230420PD202/ai-chips+components-hon-hai-research-institute-quantum-computer.html

From the Article: "Hon Hai Technology is slated to launch a 5–10 qubit open and endocable ion trap quantum computer within five years as a prototype platform for medium- and long-term scalable quantum computers, according to Guin-Dar Lin, director of the Trapped-Ion..."

How can Taiwan keep its semiconductor momentum going?

Source: https://www.digitimes.com/news/a20230420VL208/government-ic-design-ic-manufacturing-taiwan.html

From the Article: "Himax CEO Jordan Wu noted at a forum concerning Taiwan's IC design that many Taiwanese IC design houses have been able to achieve profitability. But despite the profits, they are still striving to secure government support or even trying to influence the government's policies. Why is that so? Wu pointed out that IC design is a knowledge-intensive sector that attracts global attention. Policies concerning IC design are unlike those for most other industry sectors and their making must take international competition into consideration."

Qualcomm seeking lower III-V semiconductor foundry quotes

Link back to Table of Contents
The articles have been 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/a20230419PD213/gaas-qualcomm-win-semiconductors.html

From the Article: "Qualcomm intends to increase orders for III-V semiconductor foundries capable of providing much lower quotes, according to industry sources."

AI computation needs growing faster than Moore's Law, says MediaTek exec

Source: https://www.digitimes.com/news/a20230419PD209/ai-chips+components-ic-design-distribution-mediatek-must-read.html

From the Article: "The computational demand brought about by AI model training will be the key driving force for chip growth in the future, according to B. S. Liang, senior director of the strategic technology exploration platform at MediaTek."

More than 60% of Taiwan servers exported to US

Source: https://www.digitimes.com/news/a20230417PD211/data-center-ict-manufacturing-moea-server-chip-server-demand-server-ipc-cloud-computing-iot-taiwan-us.html

From the Article: "Nearly 65% of Taiwan-made servers were bound for the US between January and March, according to data from Taiwan's Ministry of Economic Affairs (MOEA)."

Western Digital Hackers Demand 8-Figure Ransom Payment for Data

Source: https://www.darkreading.com/vulnerabilities-threats/hackers-hold-data-hostage-demanding-8-figure-ransom-payment

From the Article: "Western Digital has yet to comment on claims that the breach reported earlier this month led to data being stolen."

Balancing cybersecurity with business priorities: Advice for Boards

Source: https://www.helpnetsecurity.com/2023/04/18/alicja-cade-google-cybersecurity-business-priorities/

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

From the Article: "In today's rapidly evolving technological landscape, it's more important than ever for Boards and executives to stay informed about the latest advancements and potential risks in technology and digital capability."

China sourcing tied to largest supply chain risks of 2023: report

Source: https://www.supplychaindive.com/news/china-sourcing-supply-chain-risks-everstream-2023/647602/

From the Article: "Sourcing from Chinese manufacturers is chief among supply chain risks in 2023, according to analytics firm Everstream's annual risk report."

Conversational Attacks Fastest Growing Mobile Threat

Source: https://www.infosecurity-magazine.com/news/conversational-attacks-fastest/

From the Article: "Pig butchering and similar scams could soon be AI-driven."

Security beyond software: The open source hardware security evolution

Source: https://www.helpnetsecurity.com/2023/04/19/open-source-hardware-security/

From the Article: "Mention IT security, and most people immediately think of software-based protections against software-based threats: ransomware, viruses, and other forms of malware."

A Vision and Strategy for the National Semiconductor Technology Center
Source: https://www.nist.gov/chips/vision-and-strategy-national-semiconductor-technology-center

From the Article: "This is introductory text from the CHIPS Research and Development Office's "A Vision and Strategy for the National Semiconductor Technology Center.""

Enforcement of Cybersecurity Regulations: Part 3

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

Source: https://www.lawfareblog.com/enforcement-cybersecurity-regulations-part-3

Summary: tactics for enforcement of cybersecurity regulations

Waiting for quantum computers to arrive, software engineers get creative

Source: https://www.reuters.com/technology/waiting-quantum-computers-arrive-software-engineers-get-creative-2023-04-17/

From the Article: "OAKLAND, Calif., April 17 (Reuters) - Quantum computers promise to be millions of times faster than today's fastest supercomputers, potentially revolutionizing everything from medical research to the way people solve problems of climate change. The wait for these machines, though, has been long, despite the billions poured into them."

Post-Quantum Cryptography: the Good, the Bad, and the Powerful
Source: https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms

From the Article: "Once access to practical quantum computers becomes available, all public-key algorithms and associated protocols will be vulnerable to criminals, competitors, and other adversaries. It is critical to begin planning for the replacement of hardware, software, and services that use public-key algorithms now so that information is protected from future attacks."

Threat Actors Rapidly Adopt Web3 IPFS Technology

Source: https://unit42.paloaltonetworks.com/ipfs-used-maliciously/

From the Article: "Web3 technologies are seeing widespread adoption — including by TAs. We discuss Web3 technology InterPlanetary File System (IPFS), and malicious use of it."

Unit 42 Unveils Most 'Expansive' Cloud Threat Research Yet: Cloud Threat Report Volume 7 Examines the Expanding Attack Surface

Source: https://unit42.paloaltonetworks.com/cloud-threat-report-expanding-attack-surface/

Link back to Table of Contents

The articles have been 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 Unit 42 Cloud Threat Report, Volume 7, highlights real-world data on the state of the cloud in the cybersecurity industry."

SIA Applauds House Introduction of Bipartisan Legislation to Restore Immediate Deductibility of R&D Investments

Source: https://www.semiconductors.org/sia-applauds-house-introduction-of-bipartisan-legislation-to-restore-immediate-deductibility-of-rd-investments/?utm_content=245752105&utm_medium=social&utm_source=linkedin&hss_channel=lcp-1940570

From the Article: "WASHINGTON—April 18, 2023—The Semiconductor Industry Association (SIA) today released the following statement from SIA President and CEO John Neuffer commending the introduction in the House of Representatives of bipartisan legislation to restore full tax deductibility of R&D investments. The legislation, the American Innovation and R&D Competitiveness Act, was introduced in the House today by Reps. Ron Estes (R-Kan.) and John Larson (D-Conn.), along with more than 60 bipartisan supporters. A similar bill to restore R&D expensing was introduced in the Senate on March 16 by Sens. Maggie Hassan (D-N.H.) and Todd Young (R-Ind.) and has garnered 20 bipartisan cosponsors."

Microsoft reportedly working on its own AI chips that may rival Nvidia's

Source: https://www.theverge.com/2023/4/18/23687912/microsoft-athena-ai-chips-nvidia

From the Article: "The AI race has tech companies scrambling for Nvidia GPUs and Microsoft reportedly accelerating its own on in-house AI chips."

Supply chain executives not yet seeing expected results from technology investments

Source: https://www.supplychainquarterly.com/articles/7806-supply-chain-executives-not-yet-seeing-expected-results-from-technology-investments

From the Article: "Despite all the focus on digitalization of the supply chain, 83% of 305 executives surveyed by the consulting company PwC say that their supply chain technology investments have not fully delivered expected results. The reasons, according to "PwC's 2023 Digital Trends in Supply Chain Survey," range from the

Link back to Table of Contents

implementation process not yet being finished and it therefore being too early yet to judge results (21%) to undefined ownership and vision (4%)."

Multi-hazard risk to global port infrastructure and resulting trade and logistics losses

Source: https://www.nature.com/articles/s43247-022-00656-7

From the Article: "Despite their economic importance, the risk that ports face from multiple natural hazards has not yet been monetised on a global scale. Here, we perform an asset-level risk analysis of global port infrastructure from multiple hazards, quantifying the risk to physical asset damages and logistics services (i.e. port-specific risk) and maritime trade flows at-risk (i.e. trade risk). We find that 86% majority of ports are exposed to more than three hazards."

State Dept cyber bureau plans to add tech experts to every embassy by next year | Federal News Network

Source: https://federalnewsnetwork.com/cybersecurity/2023/04/state-dept-cyber-bureau-plans-to-add-tech-experts-to-every-embassy-by-next-year/

From the Article: "The State Department's Bureau of Cyberspace and Digital Policy is on a mission to give diplomats across the world greater access to experts in emerging technology. Ambassador at Large for Cyberspace and Digital Policy Nathaniel Fick told reporters Wednesday that the bureau plans to put a trained cyber and digital officer in every embassy around the world by the end of next year."

Cyber-attack protection bill signed into law | News | nbcrightnow.com

Source: https://www.nbcrightnow.com/news/cyber-attack-protection-bill-signed-into-law/article_1615038c-e093-11ed-b04c-af037f54546c.html

From the Article: "A committee to create a plan against cybersecurity threats will be created after Governor Jay Inslee signed Senate Bill 5518."

How to beat nation state ransomware attackers at their own game - TechRadar

Source: https://www.techradar.com/opinion/how-to-beat-nation-state-ransomware-

attackers-at-their-own-game

From the Article: "For nation states, operating in cyberspace is somewhat akin to opening Pandora's box. The benefits of global connectivity are there for all to see, but the cloak of invisibility – and deniability – that it affords hackers is very difficult to circumvent. Launching a physical attack as an act of war is difficult without someone recognizing you, but many cyber-attacks are near impossible to trace back to the source."

Ransomware rise - Professional Security Magazine

Source: https://professionalsecurity.co.uk/news/transport/ransomware-rise/

From the Article: "Aviation, maritime, rail and road transport organisations are experiencing increased levels of ransomware activity – as per ENISA's recent report. In comparison to the 13 per cent jump in total UK attack figures across all sectors from 2021 to 2022, European-wide reported ransomware attacks against the transport sector rose by a massive 41pc in 2022. But why such a large rise in attacks on this specific sector? Primarily, transport sector organisations have a distinctive profile from an attacker's perspective, making them a lucrative prospect."

Global Ransomware Protection Market Size, Share Covered Major Segments, Regions and ...

Source: https://americaclosed.com/global-ransomware-protection-market-size-and-forecast/

From the Article: "Our Global Ransomware Protection market report provides companies and individuals with the most comprehensive and up-to-date information available on the market today."

Ransomware-as-a-service tops evolving global cyber risks | PropertyCasualty360

Source: https://www.propertycasualty360.com/2023/04/21/ransomware-as-a-service-tops-evolving-global-cyber-risks/

From the Article: "So far, those fears have not come to pass. Some data suggests the war has in fact caused a lull in ransomware activity, as Ukrainian and Russian hackers take up arms instead. "

Link back to Table of Contents

Two-step supply-chain attack. Plugging leaks. Belarus as a player in the cyber war. Trends ...

Source: https://thecyberwire.com/newsletters/daily-briefing/12/76

From the Article: "Trends in ransomware. Announcement. Listen to (and follow) T-Minus, the only daily space news podcast. "

32 Supplier Websites Restored Following Reported Ransomware Breach - ASI Central

Source: https://www.asicentral.com/news/newsletters/promogram/april-2023/32-supplier-websites-restored-following-reported-ransomware-breach/

From the Article: "Within six hours, nearly 50% of the sites were restored. All were back up and running within 32 hours."

Malaysia must 'innovate' chip sector as pie shrinks amid US-China rivalry

Source: https://www.scmp.com/week-asia/economics/article/3217933/malaysia-faces-pressure-innovate-chip-sector-us-china-rivalry-gives-vietnam-boost

From the Article: "Malaysia, a key node in the global semiconductor supply chain, supplies an estimated 13 per cent of demand for packaging and testing. With increasing competition from countries like Vietnam, Malaysia should 'double down' on its advantage to stay ahead, say analysts and insiders."

China's biggest fund manager raises tech bets on regulatory easing, AI boom

Source: https://www.scmp.com/business/china-business/article/3217837/chinas-biggest-fund-manager-increases-tech-stakes-meituan-tsmc-betting-regulatory-easing-ai-boom

From the Article: "Zhang Kun, who oversees US$13 billion for Guangzhou-based E Fund Management, bought more shares in online delivery giant Meituan and TSMC in the first quarter. He is betting that the worst of a regulatory crackdown on the sector is over and that an artificial intelligence boom will bolster demand for processing chips."

Link back to Table of Contents

War of words in China-South Korea row over 'egregious' Taiwan remark escalates

Source: https://www.scmp.com/news/china/diplomacy/article/3218034/beijing-summons-south-korean-envoy-over-totally-unacceptable-taiwan-comments-president-yoon

From the Article: "President Yoon Suk-yeol's comments equating Taiwan to the South and North Korea issue has sparked a war of words with Beijing. The two issues 'are completely different in nature', vice foreign minister Sun Weidong says after summoning the South Korean ambassador."

South Korea's dominance in memory chips poised to increase as US squeezes China

Source: https://www.digitimes.com/news/a20230421VL210/china-memory-chips-south-korea-us.html

From the Article: "South Korea is poised to extend its dominance over the global memory-chip market at China's expense as US export controls shift the dynamics of semiconductor supply chains, a leading industry forecaster predicts."

OSATs striving to cut wafer bank inventories

Source: https://www.digitimes.com/news/a20230420PD212/ase-osat-tsmc.html

From the Article: "OSATs are striving to offload "wafer bank" inventories stored for customers, and are generally pessimistic about their sales prospects for the second and third quarters, according to industry sources."

TSMC mulling first advanced packaging fab overseas

Source: https://www.digitimes.com/news/a20230419PD214/advanced-packaging-japan-tsmc.html

From the Article: "TSMC is mulling to setting up an advanced packaging fab in Japan, according to sources at fab toolmakers."

Link back to Table of Contents

Outlook for handset-use ICs remains uncertain, say sources

Source: https://www.digitimes.com/news/a20230418PD208/chips+components-mobile+telecom-mobile-devices-must-read-tddi.html

From the Article: "A recent rebound in demand for LCD TDDI chips from the handset sector could be short-lived because the global consumer market has remained in the doldrums, according to industry sources."

Ransomware Attack Hits Marinette Marine Shipyard, Results in Short-Term Delay of Frigate ...

Source: https://news.usni.org/2023/04/20/ransomware-attack-hits-marinette-marine-shipyard-results-in-short-term-delay-of-frigate-freedom-lcs-construction

From the Article: "The Wisconsin shipyard that builds the U.S. Navy's Freedom-class Littoral Combat Ship and the Constellation-class guided-missile frigate suffered a ransomware attack last week that delayed production across the shipyard, USNI News has learned."

[Heads Up] The New FedNow Service Opens Massive New Attack Surface

Source: https://blog.knowbe4.com/heads-up-the-new-fednow-service-opens-massive-new-attack-surface

From the Article: "You may not have heard of this service planned for July 2023, but it promises a massive new social engineering attack surface."

Phishing for Credentials in Social Media-Based Platform Linktree

Source: https://blog.knowbe4.com/phishing-for-credentials-linktree

From the Article: "Social media is designed of course to connect, but legitimate modes of doing so can be abused. One such case of abuse that's currently running involves Linktree, a kind of meta-medium for social media users with many accounts."

Link back to Table of Contents

More Companies with Cyber Insurance Are Hit by Ransomware Than Those Without

Source: https://blog.knowbe4.com/cyber-insurance-hit-by-ransomware

From the Article: "In an interesting twist, new data hints that organizations with cyber insurance may be relying on it too much, instead of shoring up security to ensure attacks never succeed."

Cyber insurer launches InsurSec solution to help SMBs improve security, risk management

Source: https://www.csoonline.com/article/3694088/cyber-insurer-launches-insursec-solution-to-help-smbs-improve-security-risk-management.html

From the Article: "Cyber insurance provider At-Bay has announced the launch of a new InsurSec solution to help small-to-mid sized businesses (SMBs) improve their security and risk management postures through their insurance policy."

What's in Your Policy: Insurance Markets and Nation State Cyberattacks

Source: https://securityintelligence.com/articles/whats-in-your-policy-insurance-markets-nation-state-cyberattacks/

From the Article: "What happens when you think you have something valuable locked away in a safe place for an emergency, only to find out it is not available when you need it? Apart from expected disappointment, panic may set in."

Coro Raises $75 Million for Mid-Market Cybersecurity Platform

Source: https://www.securityweek.com/coro-raises-75-million-for-mid-market-cybersecurity-platform/

From the Article: "Coro, an enterprise cybersecurity platform for mid-market organizations, has raised $75 million from Energy Impact Partners."

Qualys Security Updates: Cloud Agent for Windows and Mac

Link back to Table of Contents

Source: https://blog.qualys.com/vulnerabilities-threat-research/2023/04/18/qualys-security-updates-cloud-agent-for-windows-and-mac

From the Article: "As part of our commitment to transparency and keeping customers and the community informed, Qualys is publicly disclosing three CVEs pertaining to the Qualys Cloud Agent for Windows and one CVE on the Qualys Cloud Agent for Mac. "

How the Talent Shortage Impacts Cybersecurity Leadership

Source: https://securityintelligence.com/articles/how-talent-shortage-impacts-cybersecurity-leadership/

From the Article: "The lack of a skilled cybersecurity workforce stalls the effectiveness of any organization's security program. Yes, automated tools and technologies like artificial intelligence (AI) and machine learning (ML) offer a layer of support, and bringing in a managed security service provider (MSSP) provides expertise that isn't available in-house."

The Importance of Accessible and Inclusive Cybersecurity

Source: https://securityintelligence.com/articles/importance-of-accessible-inclusive-cybersecurity/

From the Article: "As the digital world continues to dominate our personal and work lives, it's no surprise that cybersecurity has become critical for individuals and organizations."

Ransomware: Every internet-connected network is at risk. Be prepared!

Source: https://www.sans.org/blog/ransomware-every-internet-connected-network-is-at-risk/

From the Article: "As ransomware attacks increase in number and severity, even the most advanced security systems can be compromised."

Intelligence Insights: April 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.

Source: https://redcanary.com/blog/intelligence-insights-april-2023/

From the Article: "Each month, the Intel team provides Red Canary customers with an analysis of trending, emerging, or otherwise important threats that we've encountered in confirmed threat detections, intelligence reporting, and elsewhere over the preceding month. We call this report our "Intelligence Insights" and share a public version of it with the broader infosec community."

These are the cybercriminal groups behind the main cyberattacks | Atalayar

Source: https://atalayar.com/en/content/these-are-cybercriminal-groups-behind-main-cyberattacks

From the Article: "Cyberattacks have become a constant in our daily lives. In recent times, we have seen how they affect hospitals, critical infrastructures, telephone operators, automotive companies, provincial councils, town councils, etc."

Hybrid Workers Make the Attack Surface More Complex - TechSpective

Source: https://techspective.net/2023/04/21/hybrid-workers-make-the-attack-surface-more-complex/

From the Article: "Digital transformation and the modern workforce posed unique challenges for cybersecurity, but the Covid-19 pandemic caused a seismic shift in the way businesses operate, with many organizations embracing remote work as a necessary response to the pandemic."

Hackers may have made off with social security numbers, birthdates, other confidential ...

Source: https://www.kvoa.com/news/local/hackers-may-have-made-off-with-social-security-numbers-birthdates-other-confidential-information-in-tusd/article_169d24b2-e005-11ed-8c8a-5f12269d186d.html

From the Article: "(KVOA) The largest school district in Southern Arizona now believes a ransomware attack may have resulted in the personal information of current and former employees, getting into the hands of hackers."

Link back to Table of Contents

Immutability to combat ransomware in 2023 | ITWeb

Source: https://www.itweb.co.za/content/KzQenqjylEVMZd2r

From the Article: "Data is the lifeblood of today's enterprises and an extremely lucrative target for attackers. Ransomware, which essentially holds data "hostage" by encrypting it until the company pays a ransom, is increasingly common and becoming more advanced daily."

Intro to phishing: simulating attacks to build resiliency

Source: https://securityaffairs.com/145100/hacking/phishing-simulating-attacks.html

From the Article: "Phishing attacks are a major threat to organizations, they remain a perennial choice of cybercriminals when it comes to hacking their victims."

Maritime Ransomware - Security - United States - Mondaq

Source: https://www.mondaq.com/unitedstates/security/1306344/maritime-ransomware

From the Article: "Ransomware is defined as a type of malicious software designed to block access to a computer system until the attacked party pays a sum of money."

Watchdog calls on DHS to clarify when tech acquisitions require cyber risk assessments

Source: https://fedscoop.com/watchdog-calls-on-dhs-to-clarify-when-tech-acquisitions-require-cyber-risk-assessments/

Summary: DHS is being suggested to clarify when tech acquisitions will require a cyber risk assessment.

MIT and Stanford researchers develop operating system with one major promise: Resisting ransomware

Source: https://cyberscoop.com/database-oriented-operating-system-rsa/

Summary: An open source - Database Operating system (DBOS) will be demoed at

Link back to Table of Contents

RSAC this year. The fundamental difference is a DBOS is backed by a database; any changes in the operating system are stored in a database table. This is a primary difference to a file-based operating system like Unix or Windows.

OIPT to supply KAUST with hardware upgrades and ALE systems, complementing ALD

Source: https://www.semiconductor-today.com/news_items/2023/apr/oipt-200423.shtml

From the Article: "UK-based Oxford Instruments Plasma Technology (OIPT) has announced an agreement with the Saudi Arabia-based King Abdullah University of Science and Technology (KAUST) Core Labs, a system of multi-disciplinary and interconnected research laboratories."

Zaraza Malware Exploits Web Browsers To Steal Stored Passwords And Data

Source: https://latesthackingnews.com/2023/04/20/zaraza-malware-exploits-web-browsers-to-steal-stored-passwords-and-data/

From the Article: "Researchers have found new malware targeting web browsers in active campaigns."

Giving a Face to the Malware Proxy Service 'Faceless'

Source: https://krebsonsecurity.com/2023/04/giving-a-face-to-the-malware-proxy-service-faceless/

From the Article: "For the past seven years, a malware-based proxy service known as "Faceless" has sold anonymity to countless cybercriminals. For less than a dollar per day, Faceless customers can route their malicious traffic through tens of thousands of compromised systems advertised on the service. "

UK government employees receive average of 2,246 malicious emails per year

Source: https://www.itsecurityguru.org/2023/04/20/uk-government-employees-receive-average-of-2246-malicious-emails-per-year/

From the Article: "Comparitech recently conducted a series of freedom-of-information

requests, which found that UK government employees received an average of 2,246 malicious emails each in 2022. The results showed that, across 250 government organisations, Comparitech estimates that 2.16 million government employees received a total of 2.75 billion malicious emails in 2022."

How to Strengthen your Insider Threat Security

Source: https://www.itsecurityguru.org/2023/04/20/how-to-strengthen-your-insider-threat-security/

From the Article: "Let's take a common scenario: an employee sends sensitive data to their personal email to work over the weekend. A security-aware one may have thought, what's the chance of someone hacking my email vs. me finishing this work by Monday? Pretty unlikely I'll get hacked, so I choose work."

Recycled Network Devices Exposing Corporate Secrets

Source: https://www.infosecurity-magazine.com/news/recycled-network-exposing/

From the Article: "ESET warns of breach risk from kit that is not properly decommissioned."

Critical Infrastructure Firms Concerned Over Insider Threat

Source: https://www.infosecurity-magazine.com/news/critical-infrastructure-concerned/

From the Article: "Financial services sector is particularly badly impacted."

#CYBERUK23: Russian Cyber Offensive Exhibits 'Unprecedented' Speed and Agility

Source: https://www.infosecurity-magazine.com/news/russian-cyber-offensive-speed/

From the Article: "Russia's cyber operations since the invasion of Ukraine have been deployed with remarkable speed and flexibility, a new NCSC report shows."

Link back to Table of Contents

NCSC Cyber Aware Campaign Spring 2023 – What you need to know!

Source: https://www.cybernewsgroup.co.uk/ncsc-cyber-aware-campaign-spring-2023-what-you-need-to-know/

From the Article: "It has recently launched the latest phase of the Cyber Aware campaign, aiming to help sole traders, micro businesses & small organisations stay safe online."

How our vital undersea infrastructure is monitored - Innovation Origins

Source: https://innovationorigins.com/en/how-our-vital-undersea-infrastructure-is-monitored/

From the Article: "The growing threat to critical undersea infrastructure demands innovative solutions and heightened vigilance."

Multi-die systems define the future of semiconductors

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."

Chipmaker Arm to make its own semiconductor: Report - ET Telecom

Source: https://telecom.economictimes.indiatimes.com/news/devices/chipmaker-arm-to-make-its-own-semiconductor-report/99705897

From the Article: "Arm will team up with manufacturing partners to develop the new semiconductor, FT said, citing people briefed on the move, adding that the company has built a new "solutions engineering" team that will lead the development of these prototype chips for mobile devices, laptops, and other electronics."

What it will look like if China launches cyberattacks in the U.S.

Link back to Table of Contents
The articles have been 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.politico.com/news/2023/04/16/chinese-hackers-military-taiwan-invasion-00092189

From the Article: "Chinese hackers are likely to target U.S. military networks and other critical infrastructure in the event of an invasion of Taiwan."

Pen Testers Need to Hack AI, but Also Question Its Existence

Source: https://www.darkreading.com/remote-workforce/pentesters-need-to-hack-ai-question-its-existence

From the Article: "Learning how to break the latest AI models is important, but security researchers should also question whether there are enough guardrails to prevent the technology's misuse."

How Zero Trust Changed the Course of Cybersecurity

Source: https://securityintelligence.com/articles/how-zero-trust-changed-cybersecurity/

From the Article: "For decades, the IT industry relied on perimeter security to safeguard critical digital assets. Firewalls and other network-based tools monitored and validated network access. However, the shift towards digital transformation and hybrid cloud infrastructure has made these traditional security methods inadequate. Clearly, the perimeter no longer exists."

Army Going All-In on Zero Trust Principles

Source: https://www.nationaldefensemagazine.org/articles/2023/4/17/army-going-all-in-on-zero-trust-principles

From the Article: "The Army is looking to quickly accelerate its campaign to consolidate and unify its various networks and do so securely under zero trust principles, senior service leaders said April 17 at a Pentagon briefing. The Army is implementing its Unified Network Plan, which will centralize services and allow personnel to log in wherever they are in the world on any device, whether it belongs to the service or the soldier. And zero trust is the way it will securely do this, officials at the briefing said."

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

Illumio Zero Trust Segmentation Dashboard Helps Ransomware Resilience | Security News

Source: https://www.securityinformed.com/news/illumio-announces-incident-response-partner-programme-co-1543574927-ga-co-1681883945-ga.1681882209.html

From the Article: "The Incident Response Partner Program is already responsible for successfully minimizing the impact of dozens of active ransomware attacks around the world by bringing Illumio's Zero Trust Segmentation (ZTS) Platform into the practice of leading digital forensic and incident response (DFIR) providers."

Cybersecurity Still 'High Risk' in GAO's Book After Over 25 years

Source: https://fcw.com/security/2023/04/cybersecurity-still-high-risk-gaos-book-after-over-25-years/385452/

From the Article: "The management of the government's IT acquisitions and operations is also on the Government Accountability Office's biennial high risk list update this year, as it has been since 2015."

Cybersecurity Consolidation — What It Is and Why You Should Care

Source: https://www.paloaltonetworks.com/blog/?p=183205

From the Article: "Global organizations face two major security challenges in today's business climate: digital transformation and macroeconomic conditions."

US Teams Up With Partner Nations to Release Smart City Cyber Guidance

Source: https://www.nextgov.com/cybersecurity/2023/04/us-teams-partner-nations-release-smart-city-cyber-guidance/385412/

From the Article: "A joint effort between the U.S., U.K., Australia, Canada and New Zealand yielded recommendations to prevent cyber attacks on increasingly digital infrastructure."

The world needs cybersecurity experts – Microsoft expands skilling effort with a focus

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

on women

Source: https://blogs.microsoft.com/on-the-issues/2023/04/19/cybersecurity-skills-initiative-expansion-nonprofits/

From the Article: "Today, Microsoft is expanding our Cybersecurity Skills Initiative to Argentina, Chile, Indonesia, and Spain, and delivering grants to nonprofits to help skill people for the cybersecurity workforce. With this expansion, we are now working in 28 countries around the world, partnering with nonprofits and other educational institutions to train the next generation of cybersecurity professionals."

Cyberattack accelerates county's modernization, cloud push - GCN

Source: https://gcn.com/cybersecurity/2023/04/cyberattack-accelerates-countys-modernization-cloud-push/385456/

From the Article: "The cyberattack that crippled part of Suffolk County, New York's government has accelerated its shift to modernized, cloud-based technology even amid employee resistance, according to the county's IT commissioner."

Supply Chain Resilience And Agility: Two Critical Sides Of The Same Coin

Source: https://semiengineering.com/supply-chain-resilience-and-agility-two-critical-sides-of-the-same-coin/?cmid=af694453-b923-4396-9bff-2f4001eaf2a5

From the Article: "Planning for the long term is important, but so is the ability to quickly adjust to disruptions."

Secure-by-Design: A 2023 Cybersecurity Prime

Source: https://securityintelligence.com/articles/secure-by-design-a-2023-cybersecurity-primer/

From the Article: "The traditional approach to security has been to get the product to market fast and worry about security later. Unfortunately, that approach has never really worked. It puts too much of the cybersecurity responsibilities on the customer and leaves many vulnerabilities primed for exploitation at any point in the supply chain. "

Link back to Table of Contents

Ransomware reinfection and its impact on businesses - Help Net Security

Source: https://www.helpnetsecurity.com/2023/04/19/ransomware-reinfection-business-impact-video/

From the Article: "Destructive ransomware attacks impact enterprises, governments, airlines, hospitals, hotels, and individuals, causing widespread system downtime, economic loss, and reputational damage."

Microsoft Vulnerability Severity Classification for Online Services Publication

Source: https://msrc.microsoft.com/blog/2023/04/microsoft-vulnerability-severity-classification-for-online-services-publication/

From the Article: "The Microsoft Security Response Center (MSRC) is always looking for ways to provide clarity and transparency around how we assess the impact of vulnerabilities reported in our products and services. "

Seagate Handed $300 Million US Government Fine, Accused of Breaking Rules With HDD Exports to Huawei

Source: https://www.techpowerup.com/307555/seagate-handed-usd-300-million-us-government-fine-accused-of-breaking-rules-with-hdd-exports-to-huawei

From the Article: "US authorities have imposed a $300 million penalty on Seagate Technology Holdings plc, a market leader in data storage solutions, for an alleged violation of export controls. The US Commerce Department has investigated the California-based company's business dealings with Chinese hardware firm Huawei Technologies Co. Limited, specifically for the sale of hard disk drives to operations within mainland China. It has found that Seagate has broken the "foreign direct product (FDP) rule" that was established by the US Government back in 2020. Seagate is said to have sold approximately 7.4 million hard drive units to Huawei after the period in which the new rulings took effect - the total value of these shipments was estimated in the region of $1.1 billion."

Assist Layers: The Unsung Heroes of EUV Lithography

Source: https://semiengineering.com/assist-layers-the-unsung-heroes-of-euv-lithography/

Link back to Table of Contents
The articles have been 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: "Various materials work in concert with the scanner, photoresist and photomasks to make EUV lithography work."

Smarter Ways To Manufacture Chips

Source: https://semiengineering.com/smarter-ways-to-manufacture-chips/

From the Article: "Early successes are spurring further investments, with a concentration on high ROI projects."

A shocking number of businesses aren't getting their data back after a ransomware attack

Source: https://www.techradar.com/news/a-shocking-number-of-businesses-arent-getting-their-data-back-after-a-ransomware-attack

From the Article: "A vast majority of businesses that pay the demand following a ransomware (opens in new tab) attack don’t end up retrieving their encrypted and stolen data, a new report has claimed."

Risk Quantification for Big Game Hunting or Double Extortion Ransomware

Source: https://securityboulevard.com/2023/04/risk-quantification-for-big-game-hunting-or-double-extortion-ransomware/

From the Article: "We recently helped a client in financial services use cyber risk quantitative analysis to plan defenses against double extortion ransomware AKA big-game hunting ransomware. These are sophisticated, high-stakes, multi-level cyber attacks, with many moving pieces, the sort of analytics challenge that plays to the strengths of the RiskLens cyber risk quantification (CRQ) platform."

Criminal Records Service still disrupted 4 weeks after hack - BBC News

Source: https://www.bbc.com/news/technology-65324125

From the Article: "Rahim Abdel-illah, in Leicester, however, who asked that his surname

be withheld, told BBC News he was still waiting for his certificate, so he could get married in Morocco, and had no idea how long it would take as it was now impossible to check the status of his application."

Securing Your Remote Workforce: How to Reduce Cyber Threats

Source: https://securityintelligence.com/articles/securing-remote-workforce-to-reduce-cyber-threats/

From the Article: "The debates have (mostly) stopped about whether remote work is here to stay. For many people, it's just the way we work today. However, even three years later, cybersecurity around remote work is still a top concern. Both companies and employees have room for improvement in terms of protecting devices, data and apps from cybersecurity threats when working remotely."increase in ransomware attacks and increased risks to sensitive data in the cloud."

Cybersecurity in the Energy Sector: Risks and Mitigation Strategies

Source: https://www.tripwire.com/state-of-security/cybersecurity-energy-sector-risks-and-mitigation-strategies

From the Article: "The demand for cybersecurity in the energy sector is often understated. There is a misconception that very little IT is involved, and much of it does not impact operations."

Nearly One-Half of IT Pros are Told to Keep Quiet About Security Breaches

Source: https://blog.knowbe4.com/it-pros-told-keep-quiet-about-security-breaches

From the Article: "At a time when cyber attacks are achieving success in varying degrees and IT pros are keeping quiet about resulting breaches, there is one specific type of attack that has them most worried."

Can this new prototype put an end to cyberattacks? - TechRadar

Source: https://www.techradar.com/news/can-this-new-prototype-put-an-end-to-cyberattacks

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

From the Article: "In a joint project developed by ARM and the University of Cambridge, world-renowned for its computer science pedigree, the prototype processor was used in experiments by various companies for six months as part of the Technology Access Programme, courtesy of Digital Catapult with support from the University of Cambridge and Arm."

Taiwan intros first public APT system to detect trace elements in advanced chips

Source: https://www.digitimes.com/news/a20230420PD201/atomic-probe-tomography-ic-manufacturing-narlabs-semiconductor-research.html

From the Article: "The Taiwan Semiconductor Research Institute (TSRI), under the National Applied Research Laboratories (NARLabs), has recently purchased atom probe tomography (APT) equipment to support the detection of trace elements in semiconductor components by academic..."

CIS packaging house Tong Hsing less optimistic about automotive demand

Source: https://www.digitimes.com/news/a20230420PD213/cis-tong-hsing.html

From the Article: "Tong Hsing Electronic Industries has revised its automotive CIS business outlook from highly optimistic to just positive, according to the packaging house."

Taiwan urges US to calm rhetoric on China chip risk - Taipei Times

Source: https://www.taipeitimes.com/News/feat/archives/2023/04/22/2003798396

From the Article: "Taiwanese officials have urged their American counterparts to tone down their rhetoric about the dangers of relying on chips made by TSMC"

IRA and CHIPS Act bringing manufacturing back to the US

Source: https://www.digitimes.com/news/a20230417VL202/chips-act-ira-us.html

From the Article: "Since the onset of the US-China trade war, Washington has launched

a series of initiatives to bring manufacturing back to India, especially the strategically significant semiconductors. Asian manufacturers, except for China, are also building manufacturing facilities and fabs in an era when globalization yields to diversified production."

Taiwan and Singapore: A comparison of their semiconductor industry strategies

Source: https://www.digitimes.com/news/a20230418VL208/editorial-semiconductor-industry-singapore-taiwan.html&chid=10

From the Article: "The semiconductor industry has taken root in Taiwan in ways that people would not have dreamed of half a century ago. The 1970s marked a decade of turmoil for Taiwan when it had to quit the UN and then sever diplomatic ties with the US and Japan. Its..."

Exclusive: China's YMTC making progress in producing advanced 3D NAND chips with local equipment

Source: https://www.scmp.com/tech/article/3217919/tech-war-chinas-top-memory-chip-maker-ymtc-making-progress-producing-advanced-3d-nand-products

From the Article: "YMTC's top secret project, which aims to use Chinese-only equipment, has placed big orders with domestic tool suppliers, including Beijing-based Naura Technology. The ramped up sourcing of local equipment comes after YMTC received fresh funding to the tune of US$7 billion from its state-backed investors, including the 'Big Fund'."

Taiwan stands to lose investment, supply chains, if PLA keeps up drills

Source: https://www.scmp.com/economy/china-economy/article/3217076/taiwan-stands-lose-investment-supply-chains-if-pla-keeps-military-drills

From the Article: "Many US companies have been revising contingency plans as cross-strait tensions rise after the latest round of People's Liberation Army (PLA) drills. Latest flare-up follows a meeting between Taiwanese President Tsai Ing-wen and US House of Representatives speaker Kevin McCarthy in California."

Link back to Table of Contents

The U.S. Government and a cybersecurity budget.

Source: https://thecyberwire.com/podcasts/caveat/169/notes

From the Article: "This week, our guest Ilona Cohen from HackerOne sits down with Ben to discuss Biden's Cyber Strategy and National Budget allocations for cybersecurity. Ben has the story of a proposed Montana state law to ban the popular social media app TikTok. Dave's got the story of the FTC taking action against an Amazon merchant who is deceiving supplement consumers."

Ukraine reports drop in cyberattacks by pro-Russian groups

Source: https://industrialcyber.co/reports/ukraine-reports-drop-in-cyberattacks-by-pro-russian-groups/

From the Article: "The State Service of Special Communications and Information Protection of Ukraine published Saturday its cyber incidents report for the first quarter of this year, showing a decrease in the number of attacks by pro-Russian groups targeting the commercial and financial sectors, the government and local authorities, and at the security and defense sectors."

Engineering Cybersecurity into U.S. Critical Infrastructure

Source: https://hbr.org/2023/04/engineering-cybersecurity-into-u-s-critical-infrastructure

From the Article: "Summary. To better protect critical infrastructure in the United States from cyberattacks, the Biden administration is calling on organizations to build defenses into the design of systems and not rely solely on IT protections. This article explains the concepts of “cyber-informed engineering” and illustrate them with examples from the water sector."

US chip exposure to China grew even more last year

Source: https://www.lightreading.com/semiconductorsnetwork-platforms/us-chip-exposure-to-china-grew-even-more-last-year/d/d-id/784025

From the Article: "It means some of these companies may be in for a hard landing this year unless they and their Chinese customers can find and exploit loopholes that allow them to continue doing business. Perhaps top of the list are the makers of fab

Link back to Table of Contents

equipment and developers of electronic design automation (EDA) software, denied opportunities in China by US export regulations announced on October 7."

China IC alliance calls for long-term planning for semiconductor industry

Source: https://www.digitimes.com/news/a20230420PD208/china-ic-design-distribution-ic-manufacturing-must-read-us-china-chip-ban.html

From the Article: "China's Integrated Circuit Industry Technology Innovation Alliance (ICTIA) has called for long-term planning for the development of the country's semiconductor industry, instead of just focusing on fixing the short-term problems arising from the ongoing..."

Drop in China's chip, tech output casts shadow on GDP recovery

Source: https://www.digitimes.com/news/a20230418VL211/china-chips+components-gdp-ic-manufacturing.html

From the Article: "China's production of key electronics declined so far this year despite a bullish rebound in the overall economy, showing the unevenness of the country's recovery."

EU must ready China sanctions: official - Taipei Times

Source: https://www.taipeitimes.com/News/front/archives/2023/04/23/2003798447

From the Article: "FOR THE PEOPLE: While condemning Chinese military exercises around Taiwan, a German lawmaker said it is up to Taiwanese to determine their future, not Beijing"

US collaboration key to security - Taipei Times

Source: https://www.taipeitimes.com/News/editorials/archives/2023/04/23/2003798441

From the Article: "Over the past two years, China has conducted high-handed military intrusions. Beijing not only poses a serious threat to the stability in the Taiwan Strait, but also antagonized the international community with its live-fire drills. Democratic

countries should be alert to the situation."

Taiwanese firms pull back in China, move elsewhere - Taipei Times

Source: https://www.taipeitimes.com/News/front/archives/2023/04/21/2003798341

From the Article: "Taiwanese companies are cutting their exposure to China just as they ramp up investment in other parts of the world in the latest sign of how growing tensions between the US and China are reshaping global supply chains."

'Get ready': Taiwan civilians train for Chinese invasion - Taipei Times

Source: https://www.taipeitimes.com/News/feat/archives/2023/04/20/2003798266

From the Article: "The classes are part of a growing Taiwanese urgency to be ready for a worst-case scenario after seeing the Ukraine war from afar and enduring two rounds of Chinese drills in the past year, including exercises that ended last week."

US-China ties set for further 'turbulence', former Chinese envoy warns

Source: https://www.scmp.com/news/china/diplomacy/article/3218054/us-china-ties-set-further-turbulence-former-ambassador-washington-cui-tiankai-warns

From the Article: "US failure to show mutual respect and keep its promises on issues like Taiwan is worsening ties with Beijing, Cui Tiankai says. US government and media playing up 'China threat' to fend off perceived threat to hegemony, adds the ambassador to Washington from 2013 to 2021."

Taiwan's export orders in free fall as global demand for its goods wanes

Source: https://www.scmp.com/economy/global-economy/article/3217754/taiwans-export-orders-log-biggest-fall-global-financial-crisis-turnaround-seen-2024

From the Article: "Seventh-straight month of falling orders for Taiwanese goods reflects weak consumer demand from both mainland China and the West. Expectation that the US economy will continue to weaken in the coming months is 'very bad news for Taiwan's semiconductor industry'."

Link back to Table of Contents

China the leader in state-sponsored cyberattacks in 2022 - TechHQ

Source: https://techhq.com/2023/04/china-the-leader-in-state-sponsored-cyberattacks-in-2022/

From the Article: "In Part 1 of this article, we spoke to Mike McLellan, Director of Intelligence at the Secureworks Counter Threat Unit about a seeming rise in reports of business email compromise being used against business in 2022 – as revealed by the Unit's annual report on the cyber-threat landscape."

Subscription Required

Chip industry slowdown will last longer than expected, manufacturers warn

Source: https://www.ft.com/content/6973aa75-0e25-49b8-b59d-5e8d38faa6b2

From the Article: "Weakening demand for automotive components compounds slumping PC and smartphone sales"

CHINA'S YMTC SET FOR CHIP COMEBACK DESPITE US EXPORT CONTROLS

Source: https://www.ft.com/content/9ad41255-dfa9-419f-9e30-0ab537ab54fd

From the Article: "Yangtze Memory Technologies Corp, China's largest memory-chip maker,
will begin production at a new plant as early as next year, boosting
Beijing's attempts to achieve self-sufficiency for its semiconductor
industry in the face of crippling US export controls."

Chatbots Are Stepping Toward Supply Chains

Source: https://www.wsj.com/articles/chatbots-are-stepping-toward-supply-chains-5661039a

From the Article: "Software companies are looking at the latest AI technology as a way to make sense of vast stores of data, improve logistics decisions"

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

TSMC's Tough Quarter Complicates Its U.S. Chip Ambitions

Source: https://www.wsj.com/articles/tsmcs-tough-quarter-complicates-its-u-s-chip-ambitions-812b57ef?mod=Searchresults_pos1&page=1

From the Article: "Company's outlook is reminder that the chip slump will last for a while"

Taiwan's TSMC Says Sales Could Slump in Current Quarter

Source: https://www.wsj.com/articles/taiwan-semiconductor-manufacturing-tsm-q1-earnings-report-2023-2ebf2836?mod=Searchresults_pos2&page=1

From the Article: "Chip maker doesn't expect recovery in its business until second half"

TSMC is How Chip Equipment Stocks Spell 'Relief'

Source: https://www.wsj.com/livecoverage/stock-market-news-today-04-20-2023/card/tsmc-is-how-chip-equipment-stocks-spell-relief--352wGjVsohrSIJf053Ed?mod=Searchresults_pos3&page=1

From the Article: "The biggest chipmaker in the world is going through a rough patch. But it can't afford to let up on its own spending, which is good news for the companies that supply it."

U.S., Allies Weigh How to Reduce Economic Ties With China

Source: https://www.wsj.com/articles/u-s-allies-weigh-how-to-reduce-economic-ties-with-china-8f5321ab?mod=Searchresults_pos4&page=1

From the Article: "Countries seek to lessen dependence on China but maintain global trade, investment"

GlobalFoundries Files Trade-Secrets Lawsuit Against IBM

Link back to Table of Contents
The articles have been 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/globalfoundries-files-trade-secrets-lawsuit-against-ibm-57e1353b?mod=Searchresults_pos5&page=1

From the Article: "Chip maker claims IBM violated intellectual-property rights"

TSMC Objects to Conditions on U.S. Chip Subsidies - What's News - WSJ Podcasts

Source: https://www.wsj.com/podcasts/whats-news/tsmc-objects-to-conditions-on-us-chip-subsidies/d51df0a6-8b0a-43cd-9253-adc99b25fc61?mod=Searchresults_pos7&page=1

From the Article: "A.M. Edition for April 19. The world's biggest contract chip maker is seeking up to $15 billion in government money as it invests in a pair of U.S. factories, according to people familiar with the situation. However, the Journal's Peter Landers says Taiwan Semiconductor is also pushing back on U.S. rules requiring it to share profits and detail its operations. Plus, Tesla prepares to report earnings after cutting EV prices yet again. Luke Vargas hosts."

Janet Yellen Says Security Comes Before Economy in U.S.-China Relationship

Source: https://www.wsj.com/articles/janet-yellen-to-say-security-comes-before-economy-in-u-s-china-relationship-234a8933?mod=Searchresults_pos8&page=1

From the Article: "U.S. curbing some ties, but 'a full separation of our economies would be disastrous for both countries'"

U.S. Begins Planning for 6G Wireless Communications

Source: https://www.wsj.com/articles/u-s-begins-planning-for-6g-wireless-communications-246868d0?mod=Searchresults_pos9&page=1

From the Article: "Biden administration aims to reassert U.S. leadership in telecom, an area where China has made gains"

Forget Macron, Europe and the U.S. See Eye-to-Eye on China's Threat

Source: https://www.wsj.com/articles/forget-macron-europe-and-the-u-s-see-eye-to-eye-

on-chinas-threat-6075673c?mod=Searchresults_pos10&page=1

From the Article: "The real obstacle to decoupling from Beijing isn't Western governments but Western companies that have bet heavily on China"

TSMC Seeks Up to $15 Billion in U.S Subsidies but Objects to Conditions - Minute Briefing - WSJ Podcasts

Source: https://www.wsj.com/podcasts/minute-briefing/tsmc-seeks-up-to-15-billion-in-us-subsidies-but-objects-to-conditions/af19f4ed-7670-49b2-8928-1b5011de01a0?mod=Searchresults_pos11&page=1

From the Article: "The U.S. Supreme Court is expected to issue an order determining the availability of the abortion pill Mifepristone. And House Speaker Kevin McCarthy says that the text of the bill raising the U.S. debt ceiling will be ready soon. Kate Bullivant hosts."

WSJ News Exclusive | TSMC Seeks Up to $15 Billion From U.S. for Chip Plants but Objects to Conditions

Source: https://www.wsj.com/articles/tsmc-seeks-up-to-15-billion-from-u-s-for-chip-plants-but-objects-to-conditions-3bf6cfc1?mod=Searchresults_pos14&page=1

From the Article: "With construction under way in Arizona, Taiwanese semiconductor maker calls some aid terms unacceptable"

U.S.-China Tensions Over Taiwan Put Pressure on Europe

Source: https://www.wsj.com/articles/u-s-china-tensions-over-taiwan-put-pressure-on-europe-64a417dd?mod=Searchresults_pos15&page=1

From the Article: "The EU is finding it harder to avoid taking a position on a potential military conflict"

Microsoft Could Inflate Google's Mobile Search Toll

Source: https://www.wsj.com/articles/microsoft-could-inflate-googles-mobile-search-toll-

2eaa979f?mod=Searchresults_pos17&page=1

From the Article: "Default status on mobile devices may be up for grabs in AI search war"

Bank Pullback Leaves Buyout Firms Starving for Bridge Loans

Source: https://www.wsj.com/articles/bank-pullback-leaves-buyout-firms-starving-for-bridge-loans-726e91de?mod=Searchresults_pos3&page=2

From the Article: "Lenders are moving away from subscription lines of credit, which are also getting more expensive for borrowers. That makes them less attractive as a way for private-equity firms to juice performance."

Kevin McCarthy Pitches the GOP's Debt Ceiling Plan - Opinion: Potomac Watch - WSJ Podcasts

Source: https://www.wsj.com/podcasts/opinion-potomac-watch/kevin-mccarthy-pitches-the-gop-debt-ceiling-plan/73dc5464-3ce1-439a-a921-e40faa080eac?mod=Searchresults_pos8&page=2

From the Article: "The House Speaker lays out the House GOP's offer to President Biden in return for voting to raise the debt ceiling. But Biden still refuses to negotiate, which will test whether McCarthy can keep his caucus together as the borrowing limit nears. "

What The Board Needs To Know

Source: https://www.wsj.com/articles/what-the-board-needs-to-know-6b87f5c0?mod=Searchresults_pos1&page=1

From the Article: "A weekly cyber risk briefing for board directors. Does your organization have a clear policy for how corporate documents should be stored and disposed of outside the office environment? Are processes and software controls in place for restricting access to sensitive documents to only those who need it? Has the board of directors conducted a tabletop exercise recently related to responding to leaked data? Only 48% of boards have ever ‘rehearsed’ for a cyber attack according to a recent WSJ Pro and NACD survey."

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

Patient Seeks to Force Hospital Network to Pay Hackers Ransom to Remove Naked Photos Online

Source: https://www.wsj.com/articles/patient-seeks-to-force-hospital-network-to-pay-hackers-ransom-to-remove-naked-photos-online-46ee754?mod=Searchresults_pos3&page=1

From the Article: "Jane Doe lawsuit asks judge to compel Lehigh Valley Health Network to pay hackers more than $5 million in a bid to have stolen photos removed from the internet"

How Companies Should Respond to Data Leaks

Source: https://www.wsj.com/articles/how-companies-should-respond-to-data-leaks-69a85e30?mod=Searchresults_pos4&page=1

From the Article: "Cybercriminals are increasingly publishing stolen data on dark websites to pressure victim organizations to pay ransoms, rather than encrypting data until a ransom is paid. Publishing data on the dark web also facilitates other attacks, especially business email compromise, by providing attackers with intelligence on organizations and individuals. To mitigate the impact of such attacks, companies should strive to understand what data has been stolen and focus on what disclosures to make to customers and regulators."

Intelligence Leaks Cast Spotlight on a Recurring Insider Threat: Tech Support

Source: https://www.wsj.com/articles/intelligence-leaks-cast-spotlight-on-a-recurring-insider-threat-tech-support-26fe17d0?mod=Searchresults_pos6&page=1

From the Article: "IT specialists like Jack Teixeira and Edward Snowden pose challenge to government control of classified information, officials say"

New York Finance Regulator to Bill Crypto Firms for Annual Supervision Fees

Source: https://www.wsj.com/articles/new-york-finance-regulator-to-bill-crypto-firms-for-annual-supervision-fees-8e436686?mod=Searchresults_pos8&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: "New rule applying to holders of so-called Bitlicense aligns crypto sector more closely with how agency assesses insurance and banking firms"

Insurers Wary of Longer-Term Costs of Cyberattacks

Source: https://www.wsj.com/articles/insurers-wary-of-longer-term-costs-of-cyberattacks-3912feaf?mod=Searchresults_pos9&page=1

From the Article: "Claims from a single incident can stretch on for years in class-action lawsuits and investigations. Insurers are still coming to grips with how far-reaching the damage can be"

Leak of Government Secrets Adds Pressure to Overhaul Security Clearances

Source: https://www.wsj.com/articles/leak-of-government-secrets-adds-pressure-to-overhaul-security-clearances-4c6d86f6?mod=Searchresults_pos10&page=1

From the Article: "New U.S. government report warns inconsistent vetting procedures, backlogs are among factors that hobble security-clearance system"

How Bank Apps Know You're You

Source: https://www.wsj.com/articles/how-bank-apps-know-youre-you-f45df28f?mod=Searchresults_pos11&page=1

From the Article: "A lot goes on behind the scenes to keep you safe from hackers"

WSJ News Exclusive | Europe's Air-Traffic Agency Under Attack From Pro-Russian Hackers

Source: https://www.wsj.com/articles/europes-air-traffic-agency-under-attack-from-pro-russian-hackers-54b4514d?mod=Searchresults_pos12&page=1

From the Article: "Air traffic isn't at risk but the attack is ongoing, Eurocontrol said, amid fears about the safety of Europe's critical infrastructure"

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

Chatbots Are Stepping Toward Supply Chains

Source: https://www.wsj.com/articles/chatbots-are-stepping-toward-supply-chains-5661039a?mod=Searchresults_pos1&page=1

From the Article: "Software companies are looking at the latest AI technology as a way to make sense of vast stores of data, improve logistics decisions"

Lawmakers Look for Tough Implementation of Forced Labor Law Targeting China

Source: https://www.wsj.com/articles/lawmakers-look-for-tough-implementation-of-forced-labor-law-targeting-china-9e9b3e0e?mod=Searchresults_pos2&page=1

From the Article: "Hearing focuses on how goods from Xinjiang, targeted under a near-comprehensive import ban, continue to enter the U.S."

Apple Opens First Retail Store in India as It Looks to Country for Manufacturing

Source: https://www.wsj.com/articles/apple-opens-its-first-retail-store-in-india-7f3a7035?mod=Searchresults_pos5&page=1

From the Article: "The iPhone maker aims to diversify supply chain and boost sales in a country where it has struggled to gain traction"

Lululemon's Climate Goals Hinge on Replacing Oil With Plants

Source: https://www.wsj.com/articles/lululemons-climate-goals-hinge-on-replacing-oil-with-plants-6dda5c6a?mod=Searchresults_pos6&page=1

From the Article: "It took nearly two years for Lululemon to replace nylon in two shirts with a plant-based version"

Rocket Motor Shortage Curbs Weapons for Ukraine

Source: https://www.wsj.com/articles/lockheed-martin-lmt-q1-earnings-report-2023-db3de58?mod=Searchresults_pos7&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: "Lockheed Martin projects steady Ukraine-driven sales in 2023"

Car Dealer Markups Helped Drive Inflation, Study Finds

Source: https://www.wsj.com/articles/car-dealer-markups-helped-drive-inflation-study-finds-7c1d5a2d?mod=Searchresults_pos10&page=1

From the Article: "The money dealers charged over makers' suggested prices factored into a nearly 16% rise in the consumer-price index in recent years"

The U.S.'s $42.5 Billion High-Speed Internet Plan Hits a Snag: A Worker Shortage

Source: https://www.wsj.com/articles/high-speed-internet-plan-worker-shortage-be83a843?mod=Searchresults_pos14&page=1

From the Article: "Shortage of fiber technicians casts doubt on the White House goal to bring fast internet to every home this decade"

China Strikes Energy Deals as Its Clout Grows in Middle East

Source: https://www.wsj.com/articles/china-strikes-energy-deals-as-its-clout-grows-in-middle-east-b904e417?mod=Searchresults_pos15&page=1

From the Article: "Chinese stake in Qatari gas field is latest sign of Beijing's growing presence in the region"

U.S., Allies Weigh How to Reduce Economic Ties With China

Source: https://www.wsj.com/articles/u-s-allies-weigh-how-to-reduce-economic-ties-with-china-8f5321ab?mod=Searchresults_pos16&page=1

From the Article: "Countries seek to lessen dependence on China but maintain global trade, investment"

Link back to Table of Contents
The articles have been 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 Government Workers Strike Over Pay to Offset Inflation

Source: https://www.wsj.com/articles/canada-government-workers-strike-over-pay-to-offset-inflation-24263c6b?mod=Searchresults_pos20&page=1

From the Article: "Public-sector labor dispute emerges at delicate time as central bank seeks slower wage growth to further curb inflation"

Stakes in Sudan's War Include Russian Gold, Nile Dam, Key Shipping Lane

Source: https://www.wsj.com/articles/stakes-in-sudans-war-include-russian-gold-nile-dam-key-shipping-lane-e49c0b8?mod=Searchresults_pos4&page=2

From the Article: "Russia's paramilitary Wagner Group offers weapons, Egypt provides jets, pilots to rival generals in deadly conflict"

Russia Criticizes South Korean President's Remarks on Arms Supplies to Ukraine

Source: https://www.wsj.com/articles/russia-criticizes-south-korean-presidents-remarks-on-arms-supplies-to-ukraine-39fd34ec?mod=Searchresults_pos9&page=2

From the Article: "Kremlin says Seoul has 'taken a rather unfriendly position'"

Russia Seeks to Deplete Ukraine's Air Defenses Ahead of Kyiv's Expected Offensive

Source: https://www.wsj.com/articles/russia-seeks-to-deplete-ukraines-air-defenses-ahead-of-kyivs-expected-offensive-95e3f7f8?mod=Searchresults_pos12&page=2

From the Article: "Renewed drone barrage comes ahead of meeting between Ukraine's Western backers"

Copper Shortage Threatens Green Transition

Source: https://www.wsj.com/articles/copper-shortage-threatens-green-transition-620df1e5?mod=Searchresults_pos14&page=2

From the Article: "Challenges in opening new mines expected to leave production

Link back to Table of Contents

lagging behind rising demand"

To Get the EV Tax Credit, You Will Now Have to Buy an American Brand

Source: https://www.wsj.com/articles/want-a-tax-break-on-an-ev-youll-have-to-buy-an-american-brand-edd8883a?mod=Searchresults_pos17&page=2

From the Article: "New restrictions on qualifying for the up to $7,500 credit mean that only U.S. brands currently qualify"

Pentagon, Intelligence Agencies Face Calls for Details on Leak Probe - What's News - WSJ Podcasts

Source: https://www.wsj.com/podcasts/whats-news/pentagon-intelligence-agencies-face-calls-for-details-on-leak-probe/ab0de77a-49de-4f5e-a558-ebf93ac7e07b?mod=Searchresults_pos4&page=3

From the Article: "A.M. Edition for April 17. U.S. lawmakers say they don't understand how a low-level information technician was allowed to access classified documents and allegedly sneak state secrets out of secured facilities. Plus WSJ markets reporter Hannah Miao and national economics reporter Gabe Rubin preview the week ahead for markets as earnings season kicks off. Luke Vargas hosts. "

Rise of EVs Drives Mining Deals to Decade High

Source: https://www.wsj.com/articles/rise-of-evs-drives-mining-deals-to-decade-high-6fab9b47?mod=Searchresults_pos16&page=3

From the Article: "Mining companies have announced more than $65 billion worth of deals this year in race to add clean-energy metals"

Lithium Miners Slump as Chile Unveils State-Led Policy

Source: https://www.wsj.com/articles/lithium-miners-slump-as-chile-unveils-state-led-policy-784895a8?mod=Searchresults_pos7&page=4

From the Article: "President plans to create a state-owned company for the metal used

in electric cars"

What Is Happening in Sudan? The Fighting Explained

Source: https://www.wsj.com/articles/sudan-khartoum-military-what-is-happening-447d40e2?mod=Searchresults_pos9&page=5

From the Article: "A power struggle between generals has killed hundreds and trapped millions"

Criminals Are Using Tiny Devices to Hack and Steal Cars - WIRED

Source: https://www.wired.com/story/car-hacker-theft-can-security-roundup/

From the Article: "Employees of the US Immigration and Customs Enforcement agency (ICE) abused law enforcement databases to snoop on their romantic partners, neighbors, and business associates, WIRED exclusively revealed this week."

Newly Discovered LockBit Mac Ransomware Doesn't Work—Yet - WIRED

Source: https://www.wired.com/story/apple-mac-lockbit-ransomware-samples/

From the Article: "Security researchers are examining newly discovered Mac ransomware samples from the notorious gang LockBit, marking the first known example of a prominent ransomware group toying with macOS versions of its malware."

Higher education in the us faces a systemic crisis

Source: https://www.bloomberg.com/opinion/articles/2023-04-18/higher-education-in-the-us-faces-a-systemic-crisis?

From the Article: "If US universities and colleges are to revive and thrive, they need to rethink four fundamental principles."

Cybersecurity Nightmare in Japan Is Everyone Else's Problem Too

Link back to Table of Contents
The articles have been 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.bloomberg.com/news/features/2023-04-17/rising-cyberattacks-in-japan-show-how-us-europe-are-also-vulnerable??leadSource=uverify%20wall

From the Article: "Kojima Industries Corp. is a small company and little-known outside Japan, where it produces cup holders, USB sockets and door pockets for car interiors. But its modest role in the automotive supply chain is a critical one. And when the company was hacked in February 2022, it brought Toyota Motor Corp.'s entire production line to a screeching stop."

India's dependence on Russian oil soars to 30%

Source: https://asia.nikkei.com/Business/Markets/Commodities/India-s-dependence-on-Russian-oil-soars-to-30

From the Article: "Shift spurred by discounted prices stemming from Western sanctions"

Microsoft president warns China becoming close rival of ChatGPT

Source: https://asia.nikkei.com/Business/Technology/Microsoft-president-warns-China-becoming-close-rival-of-ChatGPT

From the Article: "AI innovation can be used to defend democracies, Brad Smith says"

China pumps $7bn into upgrading chip supply chain

Source: https://asia.nikkei.com/Business/Tech/Semiconductors/China-pumps-7bn-into-upgrading-chip-supply-chain

From the Article: "Government and industry work together amid U.S. tech export restrictions"

TSMC lowers full-year outlook on weak demand, chip surplus

Source: https://asia.nikkei.com/Business/Tech/Semiconductors/TSMC-lowers-full-year-outlook-on-weak-demand-chip-surplus

From the Article: "Chipmaker logs better-than-expected Q1, but sees slow recovery

Link back to Table of Contents

ahead"

U.S. sanctions will not halt rise of China's chip industry

Source: https://asia.nikkei.com/Opinion/U.S.-sanctions-will-not-halt-rise-of-China-s-chip-industry

From the Article: "Beijing still holds advantages while America struggles to boost domestic output"

GlobalFoundries sues IBM, says secrets shared with Japan's Rapidus

Source: https://asia.nikkei.com/Business/Tech/Semiconductors/GlobalFoundries-sues-IBM-says-secrets-shared-with-Japan-s-Rapidus

From the Article: "U.S. chip manufacturer also alleges illegal IP disclosures to Intel"

Analysis: Xi, not Trump, started on path to decoupling

Source: https://asia.nikkei.com/Editor-s-Picks/China-up-close/Analysis-Xi-not-Trump-started-on-path-to-decoupling

From the Article: "The leader's desire to be independent of U.S. influence has been consistent for 11 years"

Taiwan's top display makers cut production for consumer devices

Source: https://asia.nikkei.com/Business/Technology/Taiwan-s-top-display-makers-cut-production-for-consumer-devices

From the Article: "Weak TV and notebook demand leaves industry nursing a supply glut"

China chip event draws Applied Materials, others despite U.S. tensions

Source: https://asia.nikkei.com/Business/Tech/Semiconductors/China-chip-event-

Link back to Table of Contents

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

draws-Applied-Materials-others-despite-U.S.-tensions

From the Article: "Leading global companies eager to stay in biggest semiconductor market"

China's once-sizzling startup boom loses its stride

Source: https://asia.nikkei.com/Business/Startups/China-s-once-sizzling-startup-boom-loses-its-stride

From the Article: "State funds fill the vacuum as venture capital takes a step back"

Why China's chip industry still has power despite export curbs

Source: https://asia.nikkei.com/Spotlight/Caixin/Why-China-s-chip-industry-still-has-power-despite-export-curbs

From the Article: "Equipment companies in Japan, Netherlands likely to find ways around sanctions"

Apple's first India store, China GDP, Taiwan display show

Source: https://asia.nikkei.com/Spotlight/Your-Week-in-Asia/Apple-s-first-India-store-China-GDP-Taiwan-display-show

From the Article: "Your weekly lineup of Asia's biggest business and political events"

Russia's chip deals and Alibaba's new era

Source: https://asia.nikkei.com/techAsia/Russia-s-chip-deals-and-Alibaba-s-new-era

From the Article: "The inside story on the Asia tech trends that matter, from Nikkei Asia and the Financial Times"

Link back to Table of Contents