Weekly Security Articles 05-May-2023

Contribution Managers:
Christopher Sundberg
Kirsten Koepsel
Vanessa DiMase
Daniel DiMase

Please Take our On-Line Survey

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

Thank you!

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

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

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

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

Contents

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

The articles have been 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 | 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

Events - In-person

6G - North America's Next Frontier of Innovation and Investment

Source: https://www.nextgalliance.org/6gnextfrontier/

May 11, 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.

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-registration.html

May 23-24, 2023

Software & Supply Chain Assurance (SSCA) Forum

Source: https://csrc.nist.gov/scrm/ssca/

May 31 - June 1, 2023

13th Annual NICE Conference and Expo

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

Link back to Table of Contents

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

June 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

Auto-ISAC Europe Cybersecurity Summit — Automotive ISAC

Source: https://automotiveisac.com/2023-europe-summit

June 13 -14, 2023

Infosecurity Europe 2023

Link back to Table of Contents

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/

October 11-12, 2023

Link back to Table of Contents

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

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

Source: https://mena.cs4ca.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.

November 2023

Defense Manufacturing Conference Information

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

December 11-14, 2023

Request for Comments

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

Comments Due: June 8, 2023

NIST SP 1800-38 (Draft) - Migration to Post-Quantum Cryptography: Preparation for Considering the Implementation and Adoption of Quantum Safe Cryptography (Preliminary Draft)

Source: https://csrc.nist.gov/publications/detail/sp/1800-38/draft

Comments due: June 8, 2023

Implementing Data Classification Practices: NIST SP 1800-39A Prelim Draft

Source: https://csrc.nist.gov/News/2023/implementing-data-class-practices-sp-1800-39a

From the Article: "The National Cybersecurity Center of Excellence (NCCoE) has released a preliminary draft of NIST Special Publication (SP) 1800-39A, Implementing Data Classification Practices, for public comment. The public comment period for this draft is open now through June 12, 2023. See the publication details for a copy of the draft and instructions for commenting."

Comments due: June 12, 2023

CISA Requests for Comment on Secure Software Self-Attestation Form

Source: https://www.cisa.gov/news-events/alerts/2023/04/28/cisa-requests-comment-secure-software-self-attestation-form

Comments due June 26, 2023

NISTIR 8460 (Draft) - State Machine Replication and Consensus with Byzantine Adversaries

Source: https://csrc.nist.gov/publications/detail/nistir/8460/draft

Comments due: September 1, 2023

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

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

Comments due: September 30, 2023

White Paper (Draft) - Discussion Draft of the NIST Cybersecurity Framework 2.0 Core

Source: https://csrc.nist.gov/publications/detail/white-paper/2023/04/24/discussion-draft-of-the-nist-csf-20-core/draft

Comment period remains open

Link back to Table of Contents

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

Patches/Advisories

Review – 2 Advisories Published – 4-25-23
Source: https://chemical-facility-security-news.blogspot.com/2023/04/review-2-advisories-published-4-25-23.html

Abuse of the Service Location Protocol May Lead to DoS Attacks
Source: https://www.cisa.gov/news-events/alerts/2023/04/25/abuse-service-location-protocol-may-lead-dos-attacks

Scada-LTS Third Party Component
Source: https://www.cisa.gov/news-events/ics-advisories/icsa-23-115-02

CISA Releases Two Industrial Control Systems Advisories
Source: https://www.cisa.gov/news-events/alerts/2023/04/25/cisa-releases-two-industrial-control-systems-advisories

Keysight N8844A Data Analytics Web Service
Source: https://www.cisa.gov/news-events/ics-advisories/icsa-23-115-01

CISA Releases One Industrial Control Systems Medical Advisory
Source: https://www.cisa.gov/news-events/alerts/2023/04/27/cisa-releases-one-industrial-control-systems-medical-advisory

Illumina Universal Copy Service
Source: https://www.cisa.gov/news-events/ics-medical-advisories/icsma-23-117-01

Review – 1 Advisory Published 4-27-23
Source: https://chemical-facility-security-news.blogspot.com/2023/04/review-1-advisory-published-4-27-23.html

Review – Public ICS Disclosures – Week of 4-22-23
Source: https://chemical-facility-security-news.blogspot.com/2023/04/review-public-ics-disclosures-week-of-4_29.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.

CISA Adds Three Known Exploited Vulnerabilities to Catalog
Source: https://www.cisa.gov/news-events/alerts/2023/05/01/cisa-adds-three-known-exploited-vulnerabilities-catalog

Patches/Advisories Articles of Interest

Cisco Working on Patch for Vulnerability Reported by NATO Pentester

Source: https://www.securityweek.com/cisco-working-on-patch-for-vulnerability-reported-by-nato-pentester/

From the Article: "Cisco is working on a patch for an XSS vulnerability found in Prime Collaboration Deployment by a pentester from NATO’s Cyber Security Centre (NCSC)."

VMware addressed two zero-day flaws demonstrated at Pwn2Own Vancouver 2023

Source: https://securityaffairs.com/145287/security/vmware-fixes-critical-zero-days-pwn2own.html

From the Article: "VMware addressed zero-day flaws that can be chained to achieve arbitrary code execution on Workstation and Fusion software hypervisors."

Google researchers found multiple security issues in Intel TDX

Source: https://securityaffairs.com/145268/security/intel-tdx-flaws.html

From the Article: "Google Cloud Security and Project Zero researchers, working with Intel experts, discovered multiple vulnerabilities in the Intel Trust Domain Extensions (TDX)."

SLP Vulnerability Allows DoS Attacks With Amplification Factor of 2,200

Source: https://www.securityweek.com/slp-vulnerability-allows-dos-attacks-with-amplification-factor-of-2200/

From the Article: "A high-severity vulnerability in the Service Location Protocol can be exploited to launch massive DoS amplification attacks."

Organizations Warned of Security Risk in Default Apache Superset Configurations

Source: https://www.securityweek.com/organizations-warned-of-security-risk-in-default-apache-superset-configurations/

From the Article: "Attackers can exploit Apache Superset installations with default configurations to gain administrator access and execute code on servers and databases."

VMware Patches Critical Vulnerability Disclosed at Pwn2Own Hacking Contest

Source: https://www.securityweek.com/vmware-patches-critical-vulnerability-disclosed-at-pwn2own-hacking-contest/

From the Article: "VMware this week released patches for a critical vulnerability disclosed at the Pwn2Own Vancouver 2023 hacking contest."

CISA Warns of Critical Flaws in Illumina's DNA Sequencing Instruments

Source: https://thehackernews.com/2023/04/cisa-warns-of-critical-flaws-in.html

From the Article: "The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has released an Industrial Control Systems (ICS) medical advisory warning of a critical flaw impacting Illumina medical devices."

A new Mirai botnet variant targets TP-Link Archer A21

Source: https://securityaffairs.com/145278/hacking/mirai-botnet-cve-2023-1389-tp-link-archer-a21.html

From the Article: "Last week, the Zero Day Initiative (ZDI) threat-hunting team observed the Mirai botnet attempting to exploit the CVE-2023-1389 vulnerability (aka ZDI-CAN-19557/ZDI-23-451, CVSS v3: 8.8) in TP-Link Archer AX21 Wi-Fi 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.

Update Now: PaperCut Vulnerability CVE-2023-27350 Under Active Exploitation

Source: https://www.trendmicro.com/en_us/research/23/d/update-now-papercut-vulnerability-cve-2023-27350-under-active-ex.html

From the Article: "Two vulnerabilities in PaperCut have been found, and one of them is being actively exploited in the wild. This blog entry provides a summary of the vulnerabilities, and includes security guidance for IT and SOC professionals."

VMware Releases Critical Patches for Workstation and Fusion Software

Source: https://thehackernews.com/2023/04/vmware-releases-critical-patches-for.html

From the Article: "VMware has released updates to resolve multiple security flaws impacting its Workstation and Fusion software, the most critical of which could allow a local attacker to achieve code execution."

CVE-2023-20869

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-20869

From the Article: "VMware Workstation (17.x) and VMware Fusion (13.x) contain a stack-based buffer-overflow vulnerability that exists in the functionality for sharing host Bluetooth devices with the virtual machine."

CVE-2023-2293

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-2293

From the Article: "A vulnerability was found in SourceCodester Purchase Order Management System 1.0. It has been classified as problematic. This affects an unknown part of the file classes/Master.php?f=save_item."

CVE-2023-2424

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-2424

Link back to Table of Contents

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

From the Article: "A vulnerability was found in DedeCMS 5.7.106 and classified as critical. Affected by this issue is the function UpDateMemberModCache of the file uploads/dede/config.php. The manipulation leads to unrestricted upload. "

CVE-2023-2425

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-2425

From the Article: "A vulnerability was found in SourceCodester Simple Student Information System 1.0. It has been classified as problematic. This affects an unknown part of the file /classes/Master.php?f=save_course of the component Add New Course."

CVE-2023-2420

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-2420

From the Article: "A vulnerability was found in MLECMS 3.0. It has been rated as critical. This issue affects the function get_url in the library /upload/inc/lib/admin of the file upload\inc\include\common.func.php."

CVE-2023-2421

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-2421

From the Article: "A vulnerability classified as problematic has been found in Control iD RHiD 23.3.19.0. Affected is an unknown function of the file /v2/#/add/department. The manipulation of the argument Name leads to cross site scripting. It is possible to launch the attack remotely."

CVE-2023-2419

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-2419

From the Article: "A vulnerability was found in Zhong Bang CRMEB 4.6.0. It has been declared as critical. This vulnerability affects the function videoUpload of the file \crmeb\app\services\system\attachment\SystemAttachmentServices.php. The manipulation of the argument filename leads to unrestricted upload."

Link back to Table of Contents

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

CVE-2023-2417

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-2417

From the Article: "A vulnerability was found in ks-soft Advanced Host Monitor up to 12.56 and classified as problematic. Affected by this issue is some unknown functionality of the file C:\Program Files (x86)\HostMonitor\RMA-Win\rma_active.exe. The manipulation leads to unquoted search path. It is possible to launch the attack on the local host."

CVE-2023-2418

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-2418

From the Article: "A vulnerability was found in Konga 2.8.3 on Kong. It has been classified as problematic. This affects an unknown part of the component Login API. The manipulation leads to insufficiently random values. The complexity of an attack is rather high. "

CVE-2023-2408

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-2408

From the Article: "A vulnerability, which was classified as critical, has been found in SourceCodester AC Repair and Services System 1.0. Affected by this issue is some unknown functionality of the file services/view.php. The manipulation of the argument id leads to sql injection."

CVE-2023-2395

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-2395

From the Article: "A vulnerability classified as problematic has been found in Netgear SRX5308 up to 4.3.5-3. This affects an unknown part of the component Web Management Interface. The manipulation of the argument Login.userAgent leads to cross site scripting."

Link back to Table of Contents

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

CVE-2023-2397

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-2397

From the Article: "A vulnerability, which was classified as problematic, has been found in SourceCodester Simple Mobile Comparison Website 1.0. This issue affects some unknown processing of the file classes/Master.php?f=save_field. The manipulation of the argument Field Name leads to cross site scripting. The attack may be initiated remotely."

CVE-2023-25496

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-25496

From the Article: "A privilege escalation vulnerability was reported in Lenovo Drivers Management Lenovo Driver Manager that could allow a local user to execute code with elevated privileges."

CVE-2023-24269

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-24269

From the Article: "An arbitrary file upload vulnerability in the plugin upload function of Textpattern v4.8.8 allows attackers to execute arbitrary code via a crafted Zip file."

CVE-2023-30405

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-30405

From the Article: "A cross-site scripting (XSS) vulnerability in Aigital Wireless-N Repeater Mini_Router v0.131229 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the wl_ssid parameter at /boafrm/formHomeWlanSetup."

Link back to Table of Contents

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

CVE-2023-2391

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-2391

From the Article: "A vulnerability was found in Netgear SRX5308 up to 4.3.5-3 and classified as problematic. This issue affects some unknown processing of the file scgi-bin/platform.cgi?page=time_zone.htm of the component Web Management Interface."

Zyxel fixed a critical RCE flaw in its firewall devices and urges customers to install the patches

Source: https://securityaffairs.com/145416/hacking/zyxel-firewall-cve-2023-28771-rce.html

From the Article: "Researchers from TRAPA Security have discovered a critical remote code execution vulnerability, tracked as CVE-2023-28771 (CVSS score 9.8), impacting Zyxel Firewall."

Additional sources:
https://www.securityweek.com/critical-vulnerability-in-zyxel-firewalls-leads-to-command-execution/

https://thehackernews.com/2023/04/zyxel-firewall-devices-vulnerable-to.html

Numerous Vulnerabilities Spotted In Intel TDX

Source: https://latesthackingnews.com/2023/04/30/numerous-vulnerabilities-spotted-in-intel-tdx/

From the Article: "Researchers highlighted numerous security vulnerabilities affecting the Intel Trust Domain Extensions (TDX)."

Apache Superset Shipped With Unpatched RCE Vulnerability

Source: https://latesthackingnews.com/2023/04/29/apache-superset-shipped-with-unpatched-rce-vulnerability/

From the Article: "Researchers spotted a severe unpatched remote code execution vulnerability shipped by default in Apache Superset."

Link back to Table of Contents

The articles have been 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 Haven't Patched Microsoft Process Explorer, Prepare To Get Pwned

Source: https://www.theregister.com/2023/04/24/microsoft_driver_aukill_ransomware/

From the Article: "Ransomware spreaders have built a handy tool that abuses an out-of-date Microsoft Windows driver to disable security defenses before dropping malware into the targeted systems."

VMware Releases Patches For Workstation, Fusion Exploits

Source: https://www.scmagazine.com/news/vulnerability-management/vmware-releases-security-updates-fworkstation-fusion-exploits

From the Article: "VMware released security updates and workarounds on April 25 for vulnerabilities in two of its products, one of which could lead to remote code execution."

Additional sources:
https://www.malwarebytes.com/blog/news/2023/04/update-now-vmware-issues-updates-for-multiple-vulnerabilities

https://www.infosecurity-magazine.com/news/critical-flaw-patched-vmware/

Git Project Security Vulnerabilities Let Attackers Execute Arbitrary Code

Source: https://gbhackers.com/git-project-security-vulnerabilities/

From the Article: "A fresh set of Git releases was made available to fix several security flaws. It gives attackers the ability to execute arbitrary code upon successful exploitation. Upgrades are advised for all users. "

Critical VMware Vulnerabilities Let Attackers Execute Arbitrary Code

Source: https://gbhackers.com/critical-vmware-flaws/

From the Article: "VMware Workstation, Workstation Pro, and Fusion have been subjected to several privately reported and fixed flaws. VMware has published a security advisory on the critical bugs discovered and their workarounds."

TP-Link WAN-Side Vulnerability Exploited to Install Mirai Malware

Source: https://gbhackers.com/tp-link-wan-side-flaw/

From the Article: "Mirai botnet has updated its toolkit to include CVE-2023-1389, as observed by the ZDI threat-hunting team detecting new exploit attempts in Eastern Europe via their telemetry system."

Cisco Zero-Day Flaw: Let Remote Attackers Launch XSS Attacks

Source: https://gbhackers.com/cisco-zero-day-xss-flaw/

From the Article: "A zero-day flaw in Cisco's Prime Collaboration Deployment (PCD) software that can be used to launch cross-site scripting attacks has been identified. "A vulnerability in the web-based management interface of Cisco Prime Collaboration Deployment could allow an unauthenticated, remote attacker to conduct a cross-site scripting attack against a user of the interface," Cisco reports."

VMware Resolves Crucial Pwn2Own Zero-Day Exploit Chain

Source: https://informationsecuritybuzz.com/vmware-resolves-zero-day-exploit-chains/

From the Article: "To address zero-day vulnerabilities that might be used to achieve code execution on computers using unpatched versions of VMware's Workstation and Fusion software hypervisors, the company has provided security upgrades."

VMware fixes critical flaws in virtualization software (CVE-2023-20869, CVE-2023-20870)

Source: https://www.helpnetsecurity.com/2023/04/26/cve-2023-20869-cve-2023-20870/

From the Article: "VMware has fixed one critical (CVE-2023-20869) and three important flaws (CVE-2023-20870, CVE-2023-20871, CVE-2023-20872) in its VMware Workstation and Fusion virtual user session software. The former allows users to run multiple x86-based operating systems on one PC, while the latter runs Windows, Linux and other apps on Macs without having to reboot."

Link back to Table of Contents

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

Alloy Taurus Hackers Update PingPull Malware to Target Linux Systems

Source: https://www.infosecurity-magazine.com/news/alloy-taurus-update-pingpull/

From the Article: "According to Unit 42, the variant uses the same AES key as the original Windows PE malware."

Heap-based buffer overflow vulnerability in OMRON CX-Drive

Source: https://jvn.jp/en/vu/JVNVU97372625/

From the Article: "OMRON CX-Drive contains a heap-based buffer overflow vulnerability."

Git Project Security Vulnerabilities Let Attackers Execute Arbitrary Code

Source: https://gbhackers.com/git-project-security-vulnerabilities/

From the Article: "A fresh set of Git releases was made available to fix several security flaws. It gives attackers the ability to execute arbitrary code upon successful exploitation. Upgrades are advised for all users. "

Critical VMware Vulnerabilities Let Attackers Execute Arbitrary Code

Source: https://gbhackers.com/critical-vmware-flaws/

From the Article: "VMware Workstation, Workstation Pro, and Fusion have been subjected to several privately reported and fixed flaws. VMware has published a security advisory on the critical bugs discovered and their workarounds."

TP-Link WAN-Side Vulnerability Exploited to Install Mirai Malware

Source: https://gbhackers.com/tp-link-wan-side-flaw/

From the Article: "Mirai botnet has updated its toolkit to include CVE-2023-1389, as observed by the ZDI threat-hunting team detecting new exploit attempts in Eastern Europe via their telemetry system."

Cisco Discloses Zero-Day XSS Vulnerability in Prime Collaboration Deployment Software

Source: https://www.blackhatethicalhacking.com/news/cisco-discloses-zero-day-xss-vulnerability-in-prime-collaboration-deployment-software/

From the Article: "Cisco has disclosed a zero-day vulnerability in its Prime Collaboration Deployment (PCD) software that could be used for cross-site scripting attacks. The flaw was discovered in the web-based management interface of Cisco PCD 14 and earlier by a researcher at the NATO Cyber Security Centre."

VMware Issues Critical Security Updates to Fix Zero-Day Vulnerabilities

Source: https://www.blackhatethicalhacking.com/news/vmware-issues-critical-security-updates-to-fix-zero-day-vulnerabilities/

From the Article: "Virtualization software provider, VMware, has released security updates to address zero-day vulnerabilities that could potentially be used to execute code on systems running unpatched versions of the company's Workstation and Fusion software hypervisors."

Update Google Chrome (and other Chromium-based browsers) | Kaspersky official blog

Source: https://www.kaspersky.com/blog/chrome-vulnerability-april-2023/47946/

From the Article: "Another day – another browser vulnerability discovered! Indeed, the number of dangerous security holes has doubled within a week! Only recently we highlighted the urgent need to update iOS and macOS due to a major bug in Apple WebKit (the engine inside Safari and other browsers in iOS)."

CISA Warns Of PaperCut Print Software Vulnerabilities Under Attack

Source: https://latesthackingnews.com/2023/04/25/cisa-warns-of-papercut-print-software-vulnerabilities-under-attack/

Link back to Table of Contents

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

From the Article: "As described in its advisory, PaperCut has disclosed two different vulnerabilities affecting its print management software. Besides elaborating on the flaws, the firm also confirmed active exploitation of one of these vulnerabilities, as alerted by Trend Micro."

TP-Link Archer WiFi router flaw exploited by Mirai malware - Bleeping Computer

Source: https://www.bleepingcomputer.com/news/security/tp-link-archer-wifi-router-flaw-exploited-by-mirai-malware/

From the Article: "The Mirai malware botnet is actively exploiting a TP-Link Archer A21 (AX1800) WiFi router vulnerability tracked as CVE-2023-1389 to incorporate devices into DDoS (distributed denial of service) swarms."

Multiple Vulnerabilities in PaperCut NG/MF Could Allow for Remote Code Execution

Source: https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-papercut-ngmf-could-allow-for-remote-code-execution_2023-045

From the Article: "Multiple vulnerabilities have been discovered in PaperCut NG/MF, the most severe of which could allow for remote code execution. PaperCut NG/MF is a comprehensive print management system."

Multi-Vendor Online Groceries Management System 1.0 Remote Code Execution

Source: https://packetstormsecurity.com/files/171975/mvogms10-exec.txt

From the Article: "Multi-Vendor Online Groceries Management System version 1.0 suffers from a remote code execution vulnerability."

Red Hat Security Advisory 2023-1919-01

Source: https://packetstormsecurity.com/files/171966/RHSA-2023-1919-01.txt

From the Article: "Red Hat Security Advisory 2023-1919-01 - WebKitGTK is the port of the portable web rendering engine WebKit to the GTK platform. Issues addressed include code execution and use-after-free vulnerabilities."

Link back to Table of Contents

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

Red Hat Security Advisory 2023-1918-01

Source: https://packetstormsecurity.com/files/171962/RHSA-2023-1918-01.txt

From the Article: "Red Hat Security Advisory 2023-1918-01 - WebKitGTK is the port of the portable web rendering engine WebKit to the GTK platform. Issues addressed include code execution and use-after-free vulnerabilities."

Ubuntu Security Notice USN-6026-1

Source: https://packetstormsecurity.com/files/171934/USN-6026-1.txt

From the Article: "An attacker could possibly use this issue to perform illegal memory access and expose sensitive information. This issue only affected Ubuntu 20.04 LTS. It was discovered that Vim was using freed memory when dealing with regular expressions inside a visual selection. "

VMware Workspace ONE Remote Code Execution

Source: https://packetstormsecurity.com/files/171918/vmware_workspace_one_access_vmsa_2022_0011_chain.rb.txt

From the Article: "This Metasploit module combines two vulnerabilities in order achieve remote code execution in the context of the horizon user. The first vulnerability, CVE-2022-22956, is an authentication bypass in OAuth2TokenResourceController ACS which allows a remote, unauthenticated attacker to bypass the authentication mechanism and execute any operation."

VMware plugs security holes in VMware Aria Operations for Logs (CVE-2023-20864, CVE-2023-20865)

Source: https://www.helpnetsecurity.com/2023/04/24/vmware-plugs-security-holes-in-vmware-aria-operations-for-logs-cve-2023-20864-cve-2023-20865/

From the Article: "VMware has fixed two vulnerabilities (CVE-2023-20864, CVE-2023-

Link back to Table of Contents

20865) in VMware Aria Operations for Logs (formerly vRealize Log Insight), a widely used cloud solution for log analysis and management. About the vulnerabilities (CVE-2023-20864, CVE-2023-20865) CVE-2023-20864, a deserialization vulnerability, could be exploited by an unauthorized, malicious actor who has network access to VMware Aria Operations for Logs."

Podcasts/Videos

The Data Day: Tracking Cybercriminals and Nation-State Actors in the World ... - Ropes & Gray LLP

Source: https://www.ropesgray.com/en/newsroom/podcasts/2023/april/the-data-day-tracking-cybercriminals-and-nation-state-actors-in-the-world-of-cryptocurrency

Trustworthy and Ethical AI

Source: http://www.embracingdigital.org/episode-EDT135

The Importance of Testing Your Cybersecurity Response with Steve Orrin - Easy Prey Podcast

Source: https://www.easyprey.com/the-importance-of-testing-your-cybersecurity-response-with-steve-orrin/

Cyber Trooper - Episode 1: All about Pen Testing | RSS.com

Source: https://rss.com/podcasts/cybertrooper/928454/

TikTok and U.S.-China Technology Competition | ChinaPower Project

Source: https://chinapower.csis.org/podcasts/tiktok-and-u-s-china-technology-competition/

Link back to Table of Contents

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

Github, FIN7, Banks, Minecraft, Qualcomm, TenCent, BlueSky, Derek Johnson, and More – SWN #293

Source: https://www.scmagazine.com/podcast-segment/github-fin7-banks-minecraft-qualcomm-tencent-bluesky-derek-johnson-and-more-swn-293

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

Video: Everything you need to know about ongoing state-sponsored attacks targeting network infrastructure across the globe

Source: https://blog.talosintelligence.com/video-jaguar-tooth/

From the Article: "In this video, Hazel Burton interviews Matt Olney and J.J. Cummings from Talos to discuss the "Jaguar Tooth" campaign the U.K. government and other global intelligence agencies recently disclosed."

SSD AI/ML, Salsa for your Software, Hacking Smart TVs with IR, & Getting Papercuts – PSW #782

Source: https://www.scmagazine.com/podcast-segment/ssd-ai-ml-salsa-for-your-software-hacking-smart-tvs-with-ir-getting-papercuts-psw-782

Link back to Table of Contents

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

Hack All The Things With Flipper Zero – Kaitlyn Handelman – PSW #782

Source: https://www.scmagazine.com/podcast-segment/hack-all-the-things-with-flipper-zero-kaitlyn-handelman-psw-782

Simply Cyber: 🔴 April 28's Top Cyber News NOW! - Ep 355 on Apple Podcasts

Source: https://podcasts.apple.com/us/podcast/april-28s-top-cyber-news-now-ep-355/id1590662228?i=1000611061519

Simply Cyber: 🔴 April 27's Top Cyber News NOW! - Ep 354 on Apple Podcasts

Source: https://podcasts.apple.com/us/podcast/april-27s-top-cyber-news-now-ep-354/id1590662228?i=1000610963809

Simply Cyber: 🔴 April 26's Top Cyber News NOW! - Ep 353 on Apple Podcasts

Source: https://podcasts.apple.com/us/podcast/april-26s-top-cyber-news-now-ep-353/id1590662228?i=1000610779507

Simply Cyber: 🔴 April 25's Top Cyber News NOW! - Ep 352 on Apple Podcasts

Source: https://podcasts.apple.com/us/podcast/april-25s-top-cyber-news-now-ep-352/id1590662228?i=1000610591551

Simply Cyber: 🔴 April 24's Top Cyber News NOW! - Ep 351 on Apple Podcasts

Source: https://podcasts.apple.com/us/podcast/april-24s-top-cyber-news-now-ep-351/id1590662228?i=1000610435932

7MS #569: Interview with Jim Simpson of Blumira

Link back to Table of Contents

The articles have been 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://7ms.us/7ms-569-interview-with-jim-simpson-of-blumira/

An End-to-End Encryption Proposal | TWiT.TV

Source: https://twit.tv/shows/security-now/episodes/920

Is the industry ready for AI?

Source: https://thecyberwire.com/podcasts/hacking-humans/241/notes

Risky Biz News: Cl0p goes all-in on Papercut bug

Source: https://risky.biz/RBNEWS139/

Srsly Risky Biz: North Korea's "Vibes-based" targeting

Source: https://risky.biz/SRB31/

Risky Biz News: Google Authenticator can now sync data to Google accounts

Source: https://risky.biz/RBNEWS138/

Risky Business #703 -- Russia whines about its tech dependence on China

Source: https://risky.biz/RB703/

Between Two Nerds: Cyber Deterrence

Source: https://risky.biz/BTN33/

Risky Biz News: CISA will rescue abandoned open source security tool

Source: https://risky.biz/RBNEWS137/

Episode 54: How to Get Started in Cybersecurity

Source: https://www.cisecurity.org/insights/podcast/episode-54-how-to-get-started-in-cybersecurity

Tech Latest: Why is Microsoft cutting its hardware output?

Source: https://open.spotify.com/episode/1J5Hg0iK2dIvKpdJNsV5kT

What's next for experimental AI projects

Source: https://www.c4isrnet.com/video/2023/04/27/whats-next-for-experimental-ai-projects/

Understanding the role of artificial intelligence

Source: https://www.militarytimes.com/video/2023/04/27/understanding-the-role-of-artificial-intelligence/

Mark Kitz keynote speech at the C4ISRNET conference

Source: https://www.c4isrnet.com/video/2023/04/26/mark-kitz-keynote-speech-at-the-c4isrnet-conference/

The latest on software, data and artificial intelligence

Source: https://www.c4isrnet.com/video/2023/04/26/the-latest-on-software-data-and-artificial-intelligence/

space, procurement, rapid launch, hypersonics

Link back to Table of Contents

Source: https://www.c4isrnet.com/video/2023/04/26/the-us-is-rethinking-national-security-space-architecture-is-it-moving-fast-enough/

Supply-chain attack's effects spread. CISA makes new KEV entries. Bumblebee malware loader describes. Decoy Dog toolset discovered. Discord Papers were shared earlier and more widely.

Source: https://thecyberwire.com/podcasts/daily-podcast/1808/notes

From the Article: "3CX is not the only victim in the recent supply chain attack. The PaperCut critical vulnerability is under active exploitation. The Bumblebee malware loader is buzzing around in the wild. "

S3 Ep132: Proof-of-concept lets anyone hack at will

Source: https://nakedsecurity.sophos.com/2023/04/27/s3-ep132-proof-of-concept-lets-anyone-hack-at-will/

From the Article: "You can listen to us on Soundcloud, Apple Podcasts, Google Podcasts, Spotify, Stitcher and anywhere that good podcasts are found. Or just drop the URL of our RSS feed into your favourite podcatcher."

Highly sensitive data allegedly stolen from Minneapolis school district. PNP data leak caused by vulnerability, not a breach.

Source: https://thecyberwire.com/podcasts/privacy-briefing/516/notes

From the Article: "Highly sensitive data allegedly stolen from Minneapolis school district. PNP data leak caused by vulnerability, not a breach. US moves to dismiss Ken Griffin's IRS data leak lawsuit."

What's now being traded in the C2C markets. CISA would like comments on its software self-attestation form. And in Russia's hybrid war, are there cyber war crimes, or real hacktivists?

Source: https://thecyberwire.com/podcasts/daily-podcast/1812/notes

From the Article: "Cl0p and LockBit exploit PaperCut vulnerability in ransomware campaigns. Infostealer traded in the C2C market. All ads are trying to get your money, but some just take it. CISA requests comment on software self-attestation form."

BellaCiao from Tehran; PingPull from Beijing: two cyberespionage tools. SLP exploitation. Ransomware as an international threat. The state of hacktivism. Digital evidence or war crimes.

Source: https://thecyberwire.com/podcasts/daily-podcast/1810/notes

From the Article: "BellaCiao is malware from Iran's IRGC, while PingPull is malware used by the Chinese government affiliated Tarus Group. Ransomware continues to be a pervasive international threat."

Cyber Risk Quantification, Level 6 Cybersecurity, & Intel Briefing

Source: https://thecyberwire.com/podcasts/rh-isac/26/notes

From the Article: "In this episode of the Retail & Hospitality ISAC podcast, host Luke Vander Linden is joined by Cam Sabatini, senior analyst of information security, planning, and architecture at Abercrombie & Fitch Co., and Kristen Dalton, director of strategic cyber engagement, research, and analytics at RH-ISAC, as they explore cyber risk quantification (CRQ)."

BlackCat follows Cl0p to GoAnywhere. Mirai gets an upgrade. Deterring cyber war. Homeland Secrity’s cyber priorities. Action against DPRK cryptocrooks. What KillNet’s up to.

Source: https://thecyberwire.com/podcasts/daily-podcast/1809/notes

From the Article: "BlackCat (ALPHV) follows Cl0p, exploiting the GoAnywhere MFA vulnerability. The Mirai botnet exploits a vulnerability disclosed at Pwn2Own. An RSAC presentation describes US response to Russian prewar and wartime cyber operations."

VIDEO: Casino cyberattack more proof hackers are 'ramping it up' - MidlandToday.ca

Source: https://www.midlandtoday.ca/local-news/video-casino-cyberattack-more-proof-hackers-are-ramping-it-up-6897979

Link back to Table of Contents

The articles have been 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: "It's been 12 days and counting since a cyberattack forced the sudden closure of 14 casinos across Ontario, including sites in Sudbury, North Bay, Sault Ste. Marie, Wasaga Beach, Innisfil and Rama, close to Orillia."

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.”

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.

Strategic and Critical Materials Stockpiling Act Reform

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

Link back to Table of Contents

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."

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.

Link back to Table of Contents

The purpose of this case is to amend the FAR to create a new FAR part, part 40, which will be the new location for cybersecurity supply chain requirements in the FAR. Status: DARC Director tasked staff to draft final FAR rule. Report due date extended to 05/03/2023"

Standardizing Cybersecurity Requirements for Unclassified Federal Information Systems

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

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

Cyber Threat and Incident Reporting and Information Sharing

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

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

(EO) Strengthening America's Cybersecurity Workforce

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

From the Article: "Case Number 2019-014, Part Number 12, 2, 39, 52: (EO) Strengthening America's Cybersecurity Workforce. Implements Executive Order 13870 of May 2, 2019, America's Cybersecurity Workforce, which directs agencies to incorporate the NICE Framework lexicon, taxonomy and reporting requirements into 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."

Link back to Table of Contents

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

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

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

Link back to Table of Contents

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 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 date extended to 05/03/2023."

Link back to Table of Contents

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

Price, Cost and Finance - Defense Contract Finance Study

Source: https://www.acq.osd.mil/asda/dpc/pcf/finance-study.html

A Vision and Strategy for the NSTC

Source:
https://www.nist.gov/system/files/documents/2023/04/27/A%20Vision%20and%20Strategy%20for%20the%20NSTC.pdf

NSTC Vision Strategy Fact Sheet

Source: https://www.nist.gov/system/files/documents/2023/04/26/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.

DoD Releases Defense Contract Finance Study

Source: https://www.defense.gov/News/Releases/Release/Article/3357054/dod-releases-defense-contract-finance-study/

From the Article: "The Department of Defense today released the findings of its Defense Contract Finance Study, an effort to comprehensively assess the effect that DoD contract financing and profit policies have on the defense industry. Initiated in late 2019 at the recommendation of the Government Accountability Office (GAO), the study examined financial health, financing regulations, insight into the commercial marketplace, and impacts to subcontractors, including small businesses, over a 20-year timeframe."

Updating the NIST Cybersecurity Framework – Journey To CSF 2.0

Source: https://www.nist.gov/cyberframework/updating-nist-cybersecurity-framework-journey-csf-20

From the Article: "The NIST Cybersecurity Framework was intended to be a living document that is refined, improved, and evolves over time. These updates help the Framework keep pace with technology and threat trends, integrate lessons learned, and move best practice to common practice."

Source:
https://www.nist.gov/system/files/documents/2023/04/24/NIST%20Cybersecurity%20Framework%202.0%20Core%20Discussion%20Draft%204-2023%20final.pdf

Additional sources:
https://industrialcyber.co/nist/nist-csf-2-0-core-discussion-draft-released-stakeholder-feedback-invited/

Reports - Industry

How to build a Security Operations Center (on a budget)

Source: https://cybersecurity.att.com/resource-center/ebook/how-to-build-a-security-operations-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.

Cybersecurity Quarterly Spring 2023

Source: https://www.cisecurity.org/insights/white-papers/cybersecurity-quarterly-spring-2023

BCI Technology in Resilience Report 2023

Source: https://www.thebci.org/resource/bci-technology-in-resilience-report-2023.html

Mechanism Design for Improving Hardware Security Workshop Report

Source: https://cra.org/ccc/wp-content/uploads/sites/2/2023/04/01378-Mechanism-Design-Workshop-Report.pdf

Security Implications of ChatGPT | CSA

Source: https://cloudsecurityalliance.org/artifacts/security-implications-of-chatgpt/

Legislation

H.R.7677 - Supporting American Printed Circuit Boards Act of 2022

Source: https://www.congress.gov/bill/117th-congress/house-bill/7677/text?s=1&r=55

White House

Remarks by National Security Advisor Jake Sullivan on Renewing American Economic Leadership at the Brookings Institution - The White House

Source: https://www.whitehouse.gov/briefing-room/speeches-remarks/2023/04/27/remarks-by-national-security-advisor-jake-sullivan-on-renewing-american-economic-leadership-at-the-brookings-institution/

Link back to Table of Contents

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

Statement from Vice President Harris on Bosch Semiconductors Announcement - The White House

Source: https://www.whitehouse.gov/briefing-room/statements-releases/2023/04/26/statement-from-vice-president-harris-on-bosch-semiconductors-announcement/

Memorandum on Delegation of Authority Under Section 5948(d) of the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023 - The White House

Source: https://www.whitehouse.gov/briefing-room/presidential-actions/2023/04/25/memorandum-on-delegation-of-authority-under-section-5948d-of-the-james-m-inhofe-national-defense-authorization-act-for-fiscal-year-2023/

RSA Conference

#RSAC: Ransomware Poses Growing Threat to Five Eyes Nations

Source: https://www.infosecurity-magazine.com/news/ransomware-threat-five-eyes/

From the Article: "Representatives of four of the five Five Eyes nations outlined the growing threat ransomware poses and approaches to thwart it."

#RSAC: GPT-4 Empowers Cybersecurity Leaders to Make Smarter Risk Decisions

Source: https://www.infosecurity-magazine.com/news/gpt-cyber-leaders-risk-decisions/

From the Article: "SecurityScorecard has leveraged OpenAI's GPT-4 technology to help cyber leaders make faster decisions."

#RSAC: Climate Change is Increasing Cyber-Risks

Source: https://www.infosecurity-magazine.com/news/climate-change-cyber-risks/

From the Article: "Chloe Messdaghi outlines the link between climate change and increased cyber-threats, and says this topic must be addressed."

Link back to Table of Contents

#RSAC: Cyber Intrusion Campaign Against Three US Federal Agencies Thwarted

Source: https://www.infosecurity-magazine.com/news/us-federal-agencies-cyber-intrusion/

From the Article: "The CISA and CNMF prevent a foreign-based cyber-criminal carrying out an attack on three US Federal Agencies."

#RSAC: Understanding AI's Role in Cybersecurity Beyond the Hype

Source: https://www.infosecurity-magazine.com/news/ai-role-in-cybersecurity/

From the Article: "Diana Kelley explains why unrealistic expectations of AI can have serious consequences."

#RSAC: Computer Science Courses Must Teach Cybersecurity to Meet US Government Goals

Source: https://www.infosecurity-magazine.com/news/computer-science-teach/

From the Article: "The US government has for security to become a standard component of computer science courses. Infosecurity investigates how this can be achieved."

#RSAC: Organizations Warned About the Latest Attack Techniques

Source: https://www.infosecurity-magazine.com/news/orgs-warned-attack-techniques/

From the Article: "A range of experts provide insights into new techniques being used by cyber-threat actors."

#RSAC: Cyber-Attacks on Civilian Infrastructure Should Be War Crimes, says Ukraine Official

Source: https://www.infosecurity-magazine.com/news/cyberattacks-civilian/

From the Article: "Speaking during RSA, a Ukrainian official called for cyber-attacks against civilian infrastructure to be classed as war crimes."

Link back to Table of Contents

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

#RSAC: AI Dominates RSA as Excitement and Questions Surround its Potential in Cybersecurity

Source: https://www.infosecurity-magazine.com/news/ai-dominates-rsa/

From the Article: "AI tooling was one of the most dominant topics of conversation at RSA 2023 but there is still a long way to go in terms of development."

#RSAC: Securing Software Supply Chains Requires Outside-the-Box Thinking

Source: https://www.infosecurity-magazine.com/news/securing-software-supply-chains/

From the Article: "At RSA, cybersecurity experts discussed the unique nature of software supply chain attacks and approaches to tackling this growing threat."

#RSAC: Experts Urge Applying Lessons Learned from Russia-Ukraine Cyberwar to Potential China-Taiwan Scenario

Source: https://www.infosecurity-magazine.com/news/lessons-cyberwarfare-taiwan/

From the Article: "As tensions rise between China and Taiwan, US Government officials are keen to implement lessons learned from Ukraine's cyberwar."

#RSAC: ISACA's New Ransomware Incident Checklist to Aid Cyber Pros

Source: https://www.infosecurity-magazine.com/news/isaca-ransomware-incident-checklist/

From the Article: "ISACA's Rob Clyde tells Infosecurity about the role of the guidance as well as new findings about cyber insurance."

RSA Conference 2023: How hackers can fool ChatGPT's defences to create ransomware

Source: https://www.itworldcanada.com/article/rsa-conference-2023-how-hackers-can-fool-chatgpts-defences-to-create-ransomware/537733

Link back to Table of Contents

The articles have been 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: "Recent versions of ChatGPT are protected against requests to create malware. But, the RSA Conference 2023 was told Wednesday, a hacker can easily get around that with cleverly-worded requests to do much of the work of creating ransomware."

Proofpoint Introduces New Innovations at the 2023 RSA Conference to Break the Attack Chain

Source: https://www.proofpoint.com/us/newsroom/press-releases/proofpoint-introduces-new-innovations-2023-rsa-conference-break-attack-chain

From the Article: "Proofpoint, Inc., a leading cybersecurity and compliance company, today announced a host of innovations across its Aegis Threat Protection, Identity Threat Defense and Sigma Information Protection platforms, empowering organizations to stop malicious email attacks, detect and prevent identity-based threats and defend sensitive data from theft, loss and insider threats."

Delinea Onsite RSA Conference Survey Reveals Cloud Security Remains Top Cybersecurity Concern in 2023

Source: https://www.darkreading.com/application-security/delinea-onsite-rsa-conference-survey-reveals-cloud-security-remains-top-cybersecurity-concern-in-2023

From the Article: "Compliance acts as primary driver for obtaining cyber insurance, but budget constraints hinder efforts."

#RSAC: Ransomware Poses Growing Threat to Five Eyes Nations - Infosecurity Magazine

Source: https://www.infosecurity-magazine.com/news/ransomware-threat-five-eyes/

From the Article: "While speaking about how essential coalitions are to the fight against ransomware, Felicity Oswald, COO at the UK's National Cyber Security Centre (NCSC), said that in the UK ransomware is getting worse because threat actors no longer need to be skilled to hire a ransomware attack surface or methodology."

RSAC speaker offers ransomware victims unconventional advice - TechTarget

Source: https://www.techtarget.com/searchsecurity/news/365535792/RSAC-speaker-offers-ransomware-victims-unconventional-advice

From the Article: "In his session at the 2023 RSA Conference on Monday, Brandon Clark, CEO of Triton Tech Consulting in Denver, proposed a ransomware response process that works to squeeze out emotive instincts that are often tangled in the decision-making."

RSA: DoJ Makes 'Intentional' Pivot to Prioritize Cybercrime Disruption - MeriTalk

Source: https://www.meritalk.com/articles/rsa-doj-makes-intentional-pivot-to-prioritize-cybercrime-disruption/

From the Article: "U.S. Deputy Attorney General Lisa Monaco closed out day one of the RSA Conference in San Francisco by detailing the recent shift the Justice Department (DoJ) has taken to prioritize disruption when fighting cybercrime, and in the process to put victims at the center of its efforts."

#RSAC: US DoJ Prioritizes Victim Support in Cybercrime Crackdown

Source: https://www.infosecurity-magazine.com/news/doj-prioritizes-victim-support/

From the Article: "The DoJ’s Lisa Monaco urges organizations to work with the federal government following cyber-incidents."

Kemba Walden dishes on the Office of the National Cyber Director's big year

Source: https://www.scmagazine.com/analysis/application-security/kemba-walden-office-of-the-national-cyber-directors-big-year

Summary: Take-aways from an interview with Kemba Walden, the acting National Cybersecurity Director at RSAC 2023.
Software-liability - probably not in 2023, "it will take some time...because this is complicated."
Space Cybersecurity - ONCD will be concentrating on implementing SPD-5 (Trump era cybersecurity for space)

Link back to Table of Contents

The articles have been 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

Microsoft Confirms PaperCut Servers Used to Deliver LockBit and Cl0p Ransomware

Source: https://thehackernews.com/2023/04/microsoft-confirms-papercut-servers.html

From the Article: "The tech giant's threat intelligence team is attributing a subset of the intrusions to a financially motivated actor it tracks under the name Lace Tempest (formerly DEV-0950), which overlaps with other hacking groups like FIN11, TA505, and Evil Corp."

Additional sources:
https://techmonitor.ai/technology/cybersecurity/papercut-vulnerability-lockbit-clop-microsoft-ransomware

https://www.infosecurity-magazine.com/news/microsoft-blames-clop-affiliate/

https://candid.technology/papercut-server-hack-cop-lockbit-ransomware/

https://gridinsoft.com/blogs/clop-lockbit-and-papercut/

https://www.malwarebytes.com/blog/news/2023/04/update-your-papercut-application-servers-now-exploits-in-the-wild

https://www.malwarebytes.com/blog/news/2023/04/lockbit-and-cl0p-are-actively-exploiting-papercut-vulnerabilities

https://www.scmagazine.com/news/ransomware/attacks-papercut-servers-clop-lockbit-ransomware-groups

https://informationsecuritybuzz.com/microsoft-admits-papercut-servers-lockbit-cl0p-ransomware/

https://www.helpnetsecurity.com/2023/04/27/papercut-lockbit-clop/

https://www.bankinfosecurity.com/ransomware-hackers-exploit-papercut-bugs-a-21889

https://gbhackers.com/papercut-flaw/

https://www.darkreading.com/remote-workforce/attackers-abuse-papercut-rce-flaws-to-take-over-enterprise-print-servers

https://securityaffairs.com/145377/hacking/papercut-exploits-cl0p-lockbit-

Link back to Table of Contents

The articles have been 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.html

https://news.sophos.com/en-us/2023/04/27/increased-exploitation-of-papercut-drawing-blood-around-the-internet/

https://securityaffairs.com/145215/hacking/papercut-poc-exploit-code.html

https://nakedsecurity.sophos.com/2023/04/25/papercut-security-vulnerabilities-under-active-attack-vendor-urges-customers-to-patch/

https://heimdalsecurity.com/blog/papercut-flaw-exploited-to-hijack-servers-fix-released/

https://www.bleepingcomputer.com/news/security/clop-lockbit-ransomware-gangs-behind-papercut-server-attacks/

https://www.securityweek.com/microsoft-cl0p-ransomware-exploited-papercut-vulnerabilities-since-april-13/

https://www.infosecurity-magazine.com/news/microsoft-blames-clop-affiliate/

https://www.helpnetsecurity.com/2023/04/25/cve-2023-27350-poc/

Black Basta-claimed cyberattack confirmed by Yellow Pages Group | SC Media

Source: https://www.scmagazine.com/brief/ransomware/black-basta-claimed-cyberattack-confirmed-by-yellow-pages-group

From the Article: "The increased prevalence of phishing kits sourced from black markets and chatbot AI tools like ChatGPT has seen attackers quickly develop more targeted phishing campaigns."

Additional sources:
https://www.infosecurity-magazine.com/news/black-basta-hits-yellow-pages/

https://www.teiss.co.uk/news/black-basta-ransomware-group-claims-cyber-attack-on-yellow-pages-canada-leaks-stolen-data-online-12096

https://cyberintelmag.com/attacks-data-breaches/cyberattack-confirmed-by-yellow-pages-canada-as-data-from-black-basta-is-leaked/

https://www.bleepingcomputer.com/news/security/yellow-pages-canada-confirms-cyber-attack-as-black-basta-leaks-data/

Link back to Table of Contents

https://www.itechpost.com/articles/117397/20230424/canada-s-yellow-pages-confirms-data-leak-caused-black-basta.htm

https://www.malwarebytes.com/blog/news/2023/04/black-basta-ransomware-attacks-yellow-pages-canada

https://informationsecuritybuzz.com/yellow-pages-canada-alerts-of-cyberattack-as-black-basta-leaks-data/

https://cybersecuritynews.com/yellow-pages-hack-ransomware-gang-leaks-sensitive-data/

https://heimdalsecurity.com/blog/yellow-pages-canada-suffered-a-cyberattack/

This SSD has an AI chip that blocks any ransomware attack - Gearrice

Source: https://www.gearrice.com/update/this-ssd-has-an-ai-chip-that-blocks-any-ransomware-attack/

From the Article: "Cigent, a cybersecurity company, has recently introduced a new solution to protect data stored on Solid State Drives (SSDs) from hacker attacks. ransomware. The solution uses Artificial Intelligence (AI) algorithms to detect and prevent ransomware from encrypting data on the drive ssd."

Additional sources:
https://www.ruetir.com/2023/04/this-ssd-has-an-ai-chip-that-blocks-any-ransomware-attack/

https://hothardware.com/news/ssd-with-hardware-ransomware-protection

https://www.theregister.com/2023/04/24/ssd_ransomware/

https://technewsspace.com/introduced-ssd-with-hardware-anti-ransomware-protection-it-blocks-the-ssd-immediately/

https://www.tomshardware.com/news/cigent-secure-ssd-plus-ai

https://www.notebookcheck.net/Cigent-s-latest-SSDs-come-with-AI-powered-protection-against-ransomware-attacks.710144.0.html

https://www.techradar.com/news/this-ssd-reckons-its-smart-enough-to-keep-you-safe-

Link back to Table of Contents

from-ransomware-attacks

https://www.techspot.com/news/98435-new-ssd-claims-have-built-ai-powered-ransomware.html

RTM Locker Ransomware Attacks Linux, NAS, and ESXi Servers - Cyber Security News

Source: https://cybersecuritynews.com/rtm-locker-ransomware/

From the Article: "The RTM Locker ransomware gang has been discovered to utilize a Linux encryptor that focuses explicitly on virtual machines on VMware ESXi servers, making it the most recent instance of an enterprise-oriented ransomware attack."

Additional sources:
https://www.scmagazine.com/brief/uncategorized/vmware-esxi-servers-subjected-to-rtm-locker-ransomware-for-linux-attacks

https://www.infosecurity-magazine.com/news/rtm-locker-ransomware-targets-linux/

https://heimdalsecurity.com/blog/rtm-locker-ransomware-gang-targets-vmware-esxi-servers/

https://securityaffairs.com/145383/cyber-crime/linux-rtm-locker.html

https://www.securityweek.com/rtm-locker-ransomware-variant-targeting-esxi-servers/

https://techmonitor.ai/technology/cybersecurity/rtm-sells-ransomware-targeting-linux

https://www.bleepingcomputer.com/news/security/linux-version-of-rtm-locker-ransomware-targets-vmware-esxi-servers/

https://thehackernews.com/2023/04/rtm-lockers-first-linux-ransomware.html

Security leaders weigh in on CommScope breach

Source: https://www.securitymagazine.com/articles/99256-security-leaders-weigh-in-on-commscope-breach

From the Article: "Last week hackers published data stolen from CommScope through a ransomware attack. Among the stolen data was employee's Social Security numbers and bank account details."

Additional sources:
https://techcrunch.com/2023/04/27/commscope-ransomware-data/

https://hickoryrecord.com/news/local/cybersecurity-expert-talks-ransomware-in-wake-of-commscope-hacking/article_eb20a142-e504-11ed-88ae-4f0f5775a674.html

https://www.cpomagazine.com/cyber-security/vice-society-leaks-commscopes-employee-data-stolen-during-ransomware-attack/

https://www.scmagazine.com/brief/ransomware/commscopes-response-to-ransomware-attack-eludes-employees

https://informationsecuritybuzz.com/commscope-workers-left-in-the-dark-after-a-ransomware-attack/

https://hickoryrecord.com/news/local/crime-and-courts/hickory-fiber-optic-company-suffered-ransomware-attack-in-march/article_856f2c7e-e39c-11ed-9442-370f4f589009.html

New 'Atomic macOS Stealer' Malware Offered for $1,000 Per Month

Source: https://www.securityweek.com/new-atomic-macos-stealer-malware-offered-for-1000-per-month/

From the Article: "A new piece of malware named Atomic macOS Stealer (AMOS), offered for $1,000 per month, offers a wide range of data theft capabilities."

Additional sources:
https://nakedsecurity.sophos.com/2023/04/30/mac-malware-for-hire-steals-passwords-and-cryptocoins-sends-crime-logs-via-telegram/

https://gbhackers.com/hackers-selling-macos-stealer/

https://securityaffairs.com/145453/malware/atomic-macos-stealer.html

https://www.blackhatethicalhacking.com/news/new-macos-malware-atomic-for-sale-to-cybercriminals-for-1000-a-month/

https://thehackernews.com/2023/04/new-atomic-macos-stealer-can-steal-your.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://latesthackingnews.com/2023/04/30/atomic-macos-infostealer-malware-actively-targets-crypto-wallets/

Iranian 'Educated Manticore' Hackers Target Israel

Source: https://www.bankinfosecurity.com/iranian-educated-manticore-hackers-target-israel-a-21857

From the Article: "Iranian hackers are deploying an updated backdoor apparently targeting Israeli academic researchers with an interest in Iraq. A group's newly dubbed "Educated Manticore" is sending Iraq-themed bait to coax deployment of an implant known as PowerLess."

Additional sources:
https://www.darkreading.com/endpoint/educated-manticore-targets-israeli-victims-in-improved-phishing-attacks

https://research.checkpoint.com/2023/educated-manticore-iran-aligned-threat-actor-targeting-israel-via-improved-arsenal-of-tools/

https://www.infosecurity-magazine.com/news/iranian-educated-manticore-target/

https://blog.checkpoint.com/security/check-point-research-uncovers-rare-techniques-used-by-iranian-affiliated-threat-actor-targeting-israeli-entities/

https://www.csoonline.com/article/3694612/iranian-hacking-group-targets-israel-with-improved-phishing-attacks.html

3CX hack highlights risk of cascading software supply-chain compromises

Source: https://www.csoonline.com/article/3694154/3cx-hack-highlights-risk-of-cascading-software-supply-chain-compromises.html

From the Article: "At the end of March, an international VoIP software company called 3CX with over 600,000 business customers suffered a serious software supply-chain compromise that resulted in both its Windows and macOS applications being poisoned with malicious code."

Additional sources:
https://www.theregister.com/2023/04/24/in_brief_security/

Link back to Table of Contents

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

https://thecyberwire.com/stories/cad69be9e98d476c92548b85db4d5dfe/the-3cx-compromise-a-complex-supply-chain-attack

https://www.darkreading.com/attacks-breaches/2-infrastructure-organizations-further-affected-3cx-breach

https://www.helpnetsecurity.com/2023/04/24/3cx-supply-chain-compromise/

https://www.infosecurity-magazine.com/news/3cx-hackers-compromised-critical/

Personal info likely compromised following casino cyber attack: Tech expert - CTV News London

Source: https://london.ctvnews.ca/some-casino-sites-could-reopen-this-week-after-cyber-attack-but-it-may-already-be-too-late-says-tech-expert-1.6369146

From the Article: "The shutdown at Gateway Casinos caused by a cyber-attack is now into its second week, and at least one tech expert warns that it's unlikely that personal information hasn't already been compromised."

Additional sources:
https://www.casino.org/news/gateway-casinos-to-reopen-ontario-properties-after-cyberattack/

https://www.thestar.com/news/gta/2023/04/26/what-is-ransomware-a-look-at-the-malicious-software-behind-gateway-casinos-cyberattack.html

https://thesaxon.org/gateway-casinos-gradually-reopen-after-ransomware-attack/5117/

https://www.casinogamespro.com/2023/04/24/cga-official-says-local-gambling-industry-remains-resilient-despite-recent-cyberattack-against-gateway-casino-and-entertainments-business

https://www.orilliamatters.com/local-news/ransomware-attack-casino-rama-could-re-open-later-this-week-6904808

Ransomware attack reported in Spartanburg County, South Carolina - DataBreaches.net

Source: https://www.databreaches.net/ransomware-attack-reported-in-spartanburg-county-south-carolina/

From the Article: "Spartanburg County in South Carolina is responding to a ransomware attack. "

Additional sources:
https://www.foxcarolina.com/video/2023/04/28/ransomware-attack-spartanburg-county-government-computers/

https://therecord.media/south-carolina-spartanburg-county-dealing-with-ransomware-attack

https://www.foxcarolina.com/2023/04/27/computer-system-issues-impacting-spartanburg-county/

https://www.wspa.com/news/local-news/ransomware-attack-impacts-spartanburg-co-computer-network/

Iranian Charming Kitten APT used a new BellaCiao malware in recent wave of attacks

Source: https://securityaffairs.com/145354/malware/iran-charming-kitten-bellaciao.html

From the Article: "Iran-linked Charming Kitten group, (aka APT35, Phosphorus, Newscaster, and Ajax Security Team) made the headlines in 2014 when experts at iSight issued a report describing the most elaborate net-based spying campaign organized by Iranian hackers using social media."

Additional sources:
https://www.itsecurityguru.org/2023/04/28/charming-kitten-using-new-malware-in-multi-country-attacks/

https://www.tripwire.com/state-of-security/charming-kitten-targets-critical-infrastructure-us-and-elsewhere-bellaciao

https://www.darkreading.com/cloud/bellaciao-showcases-iran-threat-groups-modernizing-malware

https://thehackernews.com/2023/04/charming-kittens-new-bellaciao-malware.html

Illumina, Feds Say Genetic Testing Gear at Risk of Hacking

Source: https://www.bankinfosecurity.com/some-illumina-medical-gear-at-risk-due-to-software-flaws-a-21896

From the Article: "Federal authorities warn that hackers could take over genetic testing devices manufactured by Illumina, although neither the manufacturer nor the Food and Drug Administration has received reports of attacks. The vulnerabilities affect Illumina's Universal Copy Service software."

Additional sources:
https://thehackernews.com/2023/04/cisa-warns-of-critical-flaws-in.html

https://securityaffairs.com/145445/security/cisa-illumina-medical-devices-flaws.html

https://www.securityweek.com/fda-cisa-illumina-medical-devices-vulnerable-to-remote-hacking/

https://informationsecuritybuzz.com/severe-flaws-illumina-dna-sequencing-technology-cisa-warns/

Threat Actors Can Use Old Routers' Data to Breach Corporate Networks

Source: https://heimdalsecurity.com/blog/threat-actors-can-use-old-routers-data-to-breach-corporate-networks/

From the Article: "Discarded routers that are for sale on the secondary market are usually improperly wiped, an experiment shows. Threat actors can reboot sensitive data that haven't been completely erased from them."

Additional sources:
https://cyberintelmag.com/cloud-security/data-on-secondhand-corporate-routers-can-be-used-by-hackers-to-breach-networks/

https://www.cysecurity.news/2023/04/data-on-resold-corporate-routers-can-be.html

https://www.bleepingcomputer.com/news/security/hackers-can-breach-networks-using-data-on-resold-corporate-routers/

https://securityaffairs.com/145168/hacking/discarded-enterprise-network-equipment-risks.html

Link back to Table of Contents

Google Takes Down Cryptbot Malware Infrastructure

Source: https://www.cysecurity.news/2023/04/google-takes-down-cryptbot-malware.html

From the Article: "Google has taken down the infrastructure and distribution network linked to the Cryptbot info stealer, a malware that was being used to infect Google Chrome users and steal their data. The move comes after the tech giant filed a lawsuit against those using the malware to carry out illegal activities."

Additional sources:
https://securityaffairs.com/145396/malware/google-court-order-cryptbot-distributors.html

https://www.2-spyware.com/google-targets-cryptbot-malware-network-to-safeguard-chrome-users

https://www.scmagazine.com/news/cybercrime/google-distributors-cryptbot-malware

https://www.theregister.com/2023/04/27/google_cryptbot_shutdown/

Naivas addresses security of customers' credit & debit card info after data breach

Source: https://www.pulselive.co.ke/business/naivas-addresses-security-of-customers-credit-and-debit-card-info-after-data-breach/me4tzwl

From the Article: "In a statement signed by Naivas Chief Operating Officer Williy Kimani, the supermarket confirmed that they do not store any credit card or debit card information on their systems, and that such payment information is handled securely and protected through Secure Sockets Layer (SSL) encryption."

https://www.kahawatungu.com/naivas-confirms-data-stolen-in-ransomware-attack/

https://www.tuko.co.ke/business-economy/technology/503268-ransomware-naivas-supermarkets-system-hacked-data-stolen/

https://www.retail-insight-network.com/news/naivas-ransomware-attack-data/

'EvilExtractor' All-in-One Stealer Campaign Targets Windows User Data

Source: https://www.darkreading.com/endpoint/evilextractor-infostealer-campaign-targets-windows-os

From the Article: "An uptick in EvilExtractor activity aims to compromise endpoints to steal browser from targets across Europe and the US, researchers say."

Additional sources:
https://securityaffairs.com/145200/cyber-crime/evilextractor-info-stealer.html

https://thehackernews.com/2023/04/new-all-in-one-evilextractor-stealer.html

https://heimdalsecurity.com/blog/the-incidence-of-evilextractor-malware-rises-across-europe-and-the-u-s/

GhostToken Zero-Day Vulnerability Found In Google Cloud

Source: https://latesthackingnews.com/2023/04/24/ghosttoken-zero-day-vulnerability-found-in-google-cloud/

From the Article: "Specifically, the flaw affected the Google account application management page – the option allowing users to review the apps in use. An adversary could connect malicious apps to the account, and hide them permanently from the user. As a result, the respective Google account's user could never know the presence of the malicious app, inadvertently continuing to use an infected account."

Additional sources:
https://www.cysecurity.news/2023/04/attackers-can-hide-malicious-apps-using.html

https://gbhackers.com/ghosttoken-zero-day-flaw/

https://www.scmagazine.com/news/identity-and-access/ghosttoken-vulnerability-permanently-expose-data-google-users

Financial Services Firm NCR Hit by Ransomware Attack, Disrupting Aloha and Back Office Products

Source: https://www.cpomagazine.com/cyber-security/financial-services-firm-ncr-hit-by-ransomware-attack-disrupting-aloha-and-back-office-products/

From the Article: "A payment processing system used by over 100,000 restaurants and bars has been temporarily disrupted as its parent company, NCR, has been hit with a ransomware attack."

Additional sources:
https://www.cybersecuritydive.com/news/ncr-restores-ransomware-attack/648664/

https://www.nrn.com/technology/ncr-aloha-updates-restaurant-customers-after-ransomware-attack

https://ktvz.com/news/2023/04/24/dozens-of-new-hampshire-restaurants-affected-by-nationwide-ransomware-attack/

Symantec detects X_Trader supply chain attack affecting critical infrastructure organizations in US, Europe - Industrial Cyber

Source: https://industrialcyber.co/utilities-energy-power-water-waste/symantec-detects-x_trader-supply-chain-attack-affecting-critical-infrastructure-organizations-in-us-europe/

From the Article: "Symantec researchers disclosed Friday that a North Korean-linked operation affected more organizations beyond 3CX, including two critical infrastructure organizations in the energy sector, one in the U.S. and the other in Europe. The X_Trader software supply chain attack affected more organizations than 3CX. In addition to this, two other organizations involved in financial trading were also breached."

Additional sources:
https://cyberscoop.com/3cx-x_trader-supply-chain-north-korea/

https://www.itworldcanada.com/article/cyber-security-today-april-24-2023-the-x_trader-supply-chain-attack-may-be-more-widespread-than-initially-thought/537428

35M Downloads Of Android Minecraft Clones Spreads Adware

Source: https://informationsecuritybuzz.com/35m-downloads-minecraft-clones-adware/

From the Article: "A group of 38 Minecraft-like games on Google Play attacked devices with the Android adware “HiddenAds,” which loaded ads in the background without the user’s knowledge. "

Additional sources:
https://www.infosecurity-magazine.com/news/minecraft-clones-35-million/

Link back to Table of Contents

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

https://www.cysecurity.news/2023/04/beware-of-this-dangerous-android.html

Tangled Up: 'Tomiris' APT Uses Turla Malware, Confusing Researchers

Source: https://www.darkreading.com/threat-intelligence/tangled-up-tomiris-apt-uses-turla-malware-confusing-researchers

From the Article: "Researchers are unraveling the threads connecting two separate, but in some ways overlapping, Russian-language APTs."

Additional sources:
https://thehackernews.com/2023/04/russian-hackers-tomiris-targeting.html

https://securelist.com/tomiris-called-they-want-their-turla-malware-back/109552/

Thales Unveils CipherTrust Ransomware Protection to Safeguard Critical Data - Business Wire India

Source: https://www.businesswireindia.com/thales-unveils-ciphertrust-ransomware-protection-to-safeguard-critical-data-84242.html

From the Article: "Thales, the leading global technology and security provider, today announced the launch of its CipherTrust Transparent Encryption Ransomware Protection (CTE-RWP), an optional licensed feature to the CipherTrust Data Security Platform. CTE-RWP will elevate the protection of customer files and folders from ransomware attacks via access management controls and encryption processes."

Additional sources:
https://www.helpnetsecurity.com/2023/04/27/thales-cte-rwp/

https://financialpost.com/pmn/press-releases-pmn/business-wire-news-releases-pmn/thales-unveils-ciphertrust-ransomware-protection-to-safeguard-critical-data

UK school hit by ransomware attack - Computing

Source: https://www.computing.co.uk/news/4113037/uk-school-hit-ransomware-attack

From the Article: "A school in Wiltshire was hit by a ransomware attack last weekend.

Hardenhuish School, a mixed secondary academy in Chippenham, sent texts to parents and guardians of its 1,623 pupils notifying them of the attack."

Additional sources:
https://www.teiss.co.uk/news/news-scroller/hardenhuish-school-in-chippenham-hit-by-a-ransomware-attack-12122

https://www.infosecurity-magazine.com/news/ransomware-disrupts-network/

Cisco Launches Advanced Threat Detection XDR Platform

Source: https://gbhackers.com/cisco-xdr-platform/

From the Article: "In the recent hybrid, multi-vendor, multi-threat world, Cisco Extended Detection and Response (XDR) streamlines security operations with unrivaled visibility across the network and endpoint."

Additional sources:
https://www.darkreading.com/threat-intelligence/cisco-unveils-solution-to-rapidly-detect-advanced-cyber-threats-and-automate-response

https://www.helpnetsecurity.com/2023/04/25/cisco-xdr/

Harvard Pilgrim Health Care continues to deal with cyberattack: 'Significant impact' to members

Source: https://www.bostonherald.com/2023/04/26/harvard-pilgrim-health-care-continues-to-deal-with-cyberattack-significant-impact-to-members/

From the Article: "Harvard Pilgrim Health Care is continuing to deal with the fallout from a cyberattack that has sparked a “significant impact” to members and providers, the local health care giant said Wednesday."

Additional sources:
https://www.bostonglobe.com/2023/04/26/metro/point32health-states-second-largest-insurer-has-yet-restore-services-following-ransomware-attack/

https://www.wcvb.com/article/harvard-pilgrim-systems-ransomware-cyberattack-massachusetts/43730683

Link back to Table of Contents

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

Students' psychological reports, abuse allegations leaked by ransomware hackers

Source: https://www.nbcrightnow.com/national/students-psychological-reports-abuse-allegations-leaked-by-ransomware-hackers/article_b9da34e6-e436-11ed-aff6-3bbde6cd8331.html

From the Article: "Hackers who broke into the Minneapolis Public Schools earlier this year have circulated an enormous cache of files that appear to include highly sensitive documents on schoolchildren and teachers, including allegations of teacher abuse and students’ psychological reports."

Additional sources:
https://gizmodo.com/ransomware-gang-medusa-data-breach-minneapolis-school-a-1850380421

North Korean Hackers Target Mac Users With New 'RustBucket' Malware - SecurityWeek

Source: https://www.securityweek.com/north-korean-hackers-target-mac-users-with-new-rustbucket-malware/

From the Article: "Dubbed RustBucket and able to fetch additional payloads from its command-and-control (C&C) server, the malware has been attributed to the advanced persistent threat (APT) actor BlueNoroff, which is believed to be a subgroup of the infamous Lazarus hacking group."

Additional sources:
https://thehackernews.com/2023/04/lazarus-subgroup-targeting-apple.html

Daam Android malware can hold your phone hostage — what you need to know

Source: https://www.tomsguide.com/news/daam-android-malware-can-hold-your-phone-hostage-what-you-need-to-know

From the Article: "A new Android malware has been spotted in the wild which can bypass antivirus apps, steal loads of sensitive and financial data and even encrypt all of the files on an infected smartphone by deploying ransomware."

Additional sources: https://www.digitalinformationworld.com/2023/04/new-android-malware-daam-discovered.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.

New SLP Vulnerability Could Enable Massive DDoS Attacks

Source: https://www.infosecurity-magazine.com/news/new-slp-vulnerability-massive-ddos/

Summary: SLP was a protocol developed in the 90s to allow devices and applications to find each other. Recent vulnerabilities (CVE-2023-29552) and instances of SLP on public internet have raised to possibilities of SLP being used in a massive DDoS attack.From the article: "This includes VMWare ESXi Hypervisor, Konica Minolta printers, Planex Routers, IBM Integrated Management Module (IMM), SMC IPMI, and 665 other product types."

DEFENSE: Firewalls should be configured to filter traffic on UDP and TCP port 427 to prevent attackers from accessing SLP

Additional sources: https://gixtools.net/2023/04/new-slp-vulnerability-could-let-attackers-launch-2200x-powerful-ddos-attacks/

Ransomware is a forever problem now - One News Page

Source: https://www.onenewspage.com/n/World/1zpl8kj2ow/Ransomware-is-forever-problem-now.htm

From the Article: "Ransomware — a novelty just a few years ago — is now endemic, like COVID."

Additional sources:
https://www.axios.com/2023/04/28/ransomware-attack-cybersecurity-rsa-conference

IC Security Issues Grow, Solutions Lag

Source: https://semiengineering.com/ic-security-issues-grow-solutions-lag/

From the Article: "Signing off on hardware security may involve lifetime updates; AI adds unknowns that are difficult to trace."

Link back to Table of Contents

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

BumbleBee malware used by ransomware gangs pushed by Google ads - 2-Spyware.com

Source: https://www.2-spyware.com/bumblebee-malware-used-by-ransomware-gangs-pushed-by-google-ads

From the Article: "The world of cybersecurity is constantly changing, with new threats appearing all the time. The BumbleBee malware is one such threat, a dangerous tool used by ransomware gangs to gain initial access to networks and conduct attacks. The malware was discovered in April 2022 and is thought to have been created by the Conti team to replace the BazarLoader backdoor."

How can you do incident response if you can't recognize an incident?

Source: https://www.controlglobal.com/blogs/unfettered/blog/33004356/how-can-you-do-incident-response-if-you-cant-recognize-an-incident

From the article: "Cyber incident response starts with the assumption that you can recognize a control system cyber-related event as being a cyber event, but there's no training for the engineers to recognize an event as being cyber-related."

Nurse Call Systems, Infusion Pumps Riskiest Connected Medical Devices

Source: https://www.infosecurity-magazine.com/news/nurse-call-systems-riskiest/

Summary: Armis conducted a study on the security of medical devices; From the article: "Unsupported software issues extend to other devices as well. The Armis report suggested that 19% of all connected medical devices are running unsupported OS versions."

Cold storage giant Americold outage caused by network breach

Source: https://www.bleepingcomputer.com/news/security/cold-storage-giant-americold-outage-caused-by-network-breach/

From the article: "Americold is continuing to assess the intrusion that occurred Tues night / Wed morning. We contained the intrusion and shut down our network to ensure there is no risk to non-contained areas or customers. We are still in the discovery process on the path to rebuild the impacted systems," the cold storage giant 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.

Hacking the Layoff Process

Source: https://www.schneier.com/blog/archives/2023/04/hacking-the-layoff-process.html

Summary: A new way to avoid layoffs is by leveraging the analytics around searches done in an employee's record. An employee is less likely to be laid off if a complaint was filed against a manager, the analytics could look at that like retaliation.

T-Mobile discloses second data breach since the start of 2023

Source: https://www.bleepingcomputer.com/news/security/t-mobile-discloses-second-data-breach-since-the-start-of-2023/

Summary: The 2nd data breach in 2023 for T-Mobile impacts < 1000 customers.

Supply Chain Weekly Wrap-Up 04/14/2023-04/20/2023

Source: https://www.allthingssupplychain.com/supply-chain-weekly-wrap-up-04-14-2023-04-20-2023/

From the Article: "The European Union (EU) has finalized a €43 billion bid to increase domestic semiconductor production, in the wake of prolonged and ongoing disruption to chip supplies. The EU executive, the European Commission (EC), reached a provisional agreement on the terms of the European Chips Act, which seeks to double the EU's market share in semiconductor development, manufacturing, and material supply chains from 10% to 20% by 2030."

High burnout rate calls for supply chain leadership - Supply Chain Movement

Source: https://www.supplychainmovement.com/high-burnout-rate-calls-for-supply-chain-leadership/

From the Article: "Today's supply chain superheroes are getting tired. Since the pandemic started two and a half years ago, they have been working almost nonstop to keep the world's supply chains running. But the heavy workload is starting to take its toll. Research shows that one in three supply chain professionals show symptoms of a burnout. What can be done to reduce the workload and the associated stress?"

Link back to Table of Contents

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

Is your security organization ripe for a reorg?

Source: https://www.csoonline.com/article/3655735/is-your-security-organization-ripe-for-a-reorg.html

From the Article: "CISOs should revisit organizational structure as part of their overall strategic plans and after big shifts in enterprise needs. But experts warn that reorganizing alone isn’t a recipe for success."

Almost three-quarters of cyber attacks involve ransomware | Computer Weekly

Source: https://www.computerweekly.com/news/365535467/Almost-three-quarters-of-cyber-attacks-involve-ransomware

From the Article: "Data from Sophos’s annual Active Adversary Report reveals that almost three-quarters of the cyber security incidents it responded to in 2022 involved ransomware"

Vulnerability management vs. risk management, compared | TechTarget

Source: https://www.techtarget.com/searchsecurity/tip/Vulnerability-management-vs-risk-management-compared

From the Article: "Vulnerability management seeks out security weaknesses in an organization, while risk management involves looking holistically at how the company is running."

Operational Technology Cyberattacks and the 2023 Threat Landscape [Research]

Source: https://blogs.blackberry.com/en/2023/04/operational-technology-cyberattacks-and-2023-threat-landscape

From the Article: "The very OT (operational technology) manufacturers depend on to manage their factory floors faces an onslaught of cyberattacks that take advantage of a narrowing gap between OT and IT (information technology) networks."

Hackers Exploit Outdated WordPress Plugin to Backdoor Thousands of WordPress Sites

Source: https://thehackernews.com/2023/04/hackers-exploit-outdated-wordpress.html

From the Article: "Threat actors have been observed leveraging a legitimate but outdated WordPress plugin to surreptitiously backdoor websites as part of an ongoing campaign, Sucuri revealed in a report published last week."

Is Generative AI a Security Threat?

Source: https://www.verizon.com/about/news/generative-ai-security-threat

From the Article: "Interest in generative artificial intelligence (AI) peaked alongside a broader concern about artificial intelligence, as evidenced by an open letter urging the halt of AI research. But how real is the threat of AI? And what threat, if any, does generative AI pose, particularly in terms of cybersecurity?"

Is a US-Vietnam Strategic Partnership Likely to Happen Soon?

Source: https://thediplomat.com/2023/04/is-a-us-vietnam-strategic-partnership-likely-to-happen-soon/

From the Article: "Despite auspicious diplomatic recent developments, an upgrade of the bilateral relationship remains unlikely, at least for now."

Lazarus Continues to Evolve Tactics with Shift to Linux Malware

Source: https://www.blackhatethicalhacking.com/news/lazarus-continues-to-evolve-tactics-with-shift-to-linux-malware/

From the Article: "North Korean threat group Lazarus, notorious for its high-profile cyber attacks, has expanded its Operation DreamJob campaign to target Linux users with malware for the first time."

Check Point Software Technologies and BBT.live Join Forces to Bring Enhanced Cybersecurity to Remote Networks with Secure SD-WAN Solution

Source: https://blog.checkpoint.com/security/check-point-software-technologies-and-bbt-live-join-forces-to-bring-enhanced-cybersecurity-to-remote-networks-with-secure-sd-wan-solution/

From the Article: "At Check Point, we understand that cybersecurity is more important than ever

Link back to Table of Contents

in today's digital world. As businesses and individuals become more reliant on digital technology, they become more vulnerable to cyber threats such as hacking, phishing, and malware."

24th April – Threat Intelligence Report

Source: https://research.checkpoint.com/2023/24th-april-threat-intelligence-report/

From the Article: "Researchers have discovered that last month's 3CX Software supply chain attack was allegedly caused by an additional prior supply chain compromise. In that case, suspected North Korean attackers breached the site of stock trading automation company "Trading Technologies", to push its trojanized software builds, and among other victims to infect 3CX."

Vulnerability Spotlight: Vulnerabilities in IBM AIX could lead to command injection with elevated privileges

Source: https://blog.talosintelligence.com/vuln-spotlight-ibm-aix-privilege-escalation/

From the Article: "A Cisco security researcher recently discovered two vulnerabilities in the IBM AIX Unix platforms that could be exploited to inject commands and logs into targeted systems with elevated privileges."

Cisco's Vision to Rapidly Detect Cyber Threats and Automate Response

Source: https://feedpress.me/link/23532/16090784/cisco-security-vision-detect-cyber-threats-automate-response

From the Article: "With the growing number of attacks on public and private actors, cybersecurity has plainly grown to become a top priority for businesses and policymakers. Russia's invasion of Ukraine and new technologies have put additional pressure on policymakers to urgently resolve the European Union (EU) cybersecurity shortcomings."

Circle Security debuts platform "purpose-built" to tackle credential-driven threats, cloud attacks

Source: https://www.csoonline.com/article/3694554/circle-security-debuts-platform-purpose-built-to-tackle-credential-driven-threats-cloud-attacks.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 company Circle Security has emerged from stealth with the release of a new platform “purpose-built” to protect against credential-driven threats and cloud attacks."

Abnormal Security expands threat protection to Slack, Teams and Zoom

Source: https://www.csoonline.com/article/3694557/abnormal-security-expands-threat-protection-to-slack-teams-and-zoom.html

From the Article: "Cloud-based email security provider Abnormal Security has announced three new capabilities focusing on threat detection for Slack, Microsoft Teams, and Zoom."

Thousands of misconfigured container and artifact registries expose sensitive credentials

Source: https://www.csoonline.com/article/3694553/thousands-of-misconfigured-container-and-artifact-registries-expose-sensitive-credentials.html

From the Article: "Researchers have found thousands of publicly exposed and misconfigured container registries and artifact repositories belonging to businesses that could give attackers access to access tokens, encryption keys, and other sensitive information about internal systems."

Siemens focuses on zero trust, legacy hardware, supply chain challenges to ensure cybersecurity of internal systems

Source: https://www.csoonline.com/article/3693988/siemens-focuses-on-zero-trust-legacy-hardware-supply-chain-challenges-to-ensure-cybersecurity-of-in.html

From the Article: "Siemens has been working to be on top of vulnerabilities found in its products, but more importantly, to ensure the security of its internal operations. The manufacturing giant that works across several different lines of business, including industrial, smart infrastructure, health care, financial services, is protecting its systems by focusing on three main areas: zero trust, supply chain, and legacy systems."

Flashpoint releases Ignite platform with threat intelligence reports, rule-based alerts

Source: https://www.csoonline.com/article/3694194/flashpoint-releases-ignite-platform-with-threat-intelligence-reports-rule-based-alerts.html

Link back to Table of Contents

From the Article: "Threat intelligence firm Flashpoint has announced the release of Ignite, a new intelligence platform built to accelerate cross-functional risk mitigation and prevention across vulnerability management and security teams, including those in law enforcement, state and local government, and federal civilian agencies."

BrandPost: What 2022 taught us about DDoS attacks

Source: https://www.csoonline.com/article/3694570/what-2022-taught-us-about-ddos-attacks.html

From the Article: "Microsoft mitigated an average of 1,435 distributed denial-of-service (DDoS) attacks per day in 2022. This trend represents a significant threat for businesses, as DDoS attacks work by targeting websites and servers to disrupt network services and exhaust an application’s resources."

OT giants collaborate on ETHOS early threat and attack warning system

Source: https://www.csoonline.com/article/3694450/ot-giants-collaborate-on-ethos-early-threat-and-attack-warning-system.html

From the Article: "One of the greatest fears among government officials and security experts is a crippling cyberattack on industrial organizations that run essential services, including electricity, water, oil and gas production, and manufacturing systems."

Paladin Cloud launches new tool for attack surface discovery and management

Source: https://www.csoonline.com/article/3694353/paladin-cloud-launches-new-tool-for-attack-surface-discovery-and-management.html

From the Article: "Open source, cloud security firm Paladin Cloud has launched a new SaaS-based platform for enterprise cloud attack surface discovery and vulnerability management."

BrandPost: Cybersecurity in Finance: Protecting Your Digital Transformation

Source: https://www.csoonline.com/article/3689874/cybersecurity-in-finance-protecting-your-digital-transformation.html

From the Article: "Cyberattacks have become a global epidemic, leaving businesses asking, what does it take to stay ahead? Data breaches have the power to cause significant harm to a business' finances, customer experience, and reputation."

BrandPost: Unified Endpoint Management: A Powerful Tool for Your Cybersecurity Arsenal

Source: https://www.csoonline.com/article/3689873/unified-endpoint-management-a-powerful-tool-for-your-cybersecurity-arsenal.html

From the Article: "Welcome to the "Everywhere Workplace." It's here thanks to new mobile and cloud computing technologies that empower users to be more productive, on any device, and virtually anywhere they work."

North Dakota turns to AI to boost effectiveness and efficiency of its cybersecurity

Source: https://www.csoonline.com/article/3694089/north-dakota-turns-to-ai-to-boost-effectiveness-and-efficiency-of-its-cybersecurity.html

From the Article: "The recent proliferation of tools that employ artificial intelligence (AI) or machine learning (ML) to perform human-like tasks has sparked a great deal of interest in the cybersecurity community. And they've prompted some very hard questions about the future, not the least of which is whether ChatGPT, BardAI, Bing AI, and the dozens of other "AI" applications and tools already in use represent a threat or boon to security operations."

Cisco patches high and critical flaws across several products

Source: https://www.csoonline.com/article/3694192/cisco-patches-high-and-critical-flaws-across-several-products.html

From the Article: "Cisco fixed serious vulnerabilities across several of its products this week, including in its Industrial Network Director, Modeling Labs, ASR 5000 Series Routers, and BroadWorks Network Server. The flaws can lead to administrative command injection, authentication bypass, remote privilege escalation and denial of service."

The strong link between cyber threat intelligence and digital risk protection

Source: https://www.csoonline.com/article/3693754/the-strong-link-between-cyber-threat-intelligence-and-digital-risk-protection.html

From the Article: "While indicators of compromise (IoCs) and attackers' tactics, techniques, and processes (TTPs) remain central to threat intelligence, cyber threat intelligence (CTI) needs have grown over the past few years, driven by things like digital transformation, cloud computing, SaaS propagation, and remote worker support."

Good Friday Agreement paved way for Northern Ireland's emergence as a global cybersecurity hub

Source: https://www.csoonline.com/article/3694076/good-friday-agreement-paved-way-for-northern-ireland-s-emergence-as-a-global-cybersecurity-hub.html

From the Article: "The Belfast (Good Friday) Agreement played an integral role in enabling Northern Ireland's growth as a global cybersecurity hub, according to UK government chiefs speaking at the CyberUK conference in Belfast. The Good Friday Agreement was signed on Good Friday, April 10, 1998, following three decades of conflict known as the Troubles."

AuKill tool uses BYOVD attack to disable EDR software

Source: https://securityaffairs.com/145227/malware/aukill-tool-byovd-attack.html

From the Article: "Sophos researchers reported that threat actors are using a previously undocumented defense evasion tool, dubbed AuKill, to disable endpoint detection and response (EDR) software."

An Official Threat Notice was issued at the Govt's annual cyber security conference with Russia specifically singled out!

Source: https://www.cybernewsgroup.co.uk/an-official-threat-notice-was-issued-at-the-govts-annual-cyber-security-conference-with-russia-specifically-singled-out/

From the Article: "The National Cyber Security Centre (NCSC) – a part of GCHQ – has released a new report warning 1,000s of people are almost certainly already being targeted yearly through the "irresponsible use of spyware.""

Link back to Table of Contents

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

Russian Cyberattacks on Ukraine’s Private Sector Worsen!

Source: https://www.cybernewsgroup.co.uk/russian-cyberattacks-on-ukraines-private-sector-worsen/

From the Article: "In the 1st quarter of 2023 the Computer Emergency Response Team of Ukraine (CERT-UA) noticed an increased number of attacks on the country’s commercial organisations. CERT-UA attributed the increase to private companies implementing new solutions on their systems."

Weekly Cyber Threat Report, April 17 – 21, 2023

Source: https://cyberintelmag.com/threat-intelligence/weekly-cyber-threat-report-april-17-21-2023/

From the Article: "This week’s good news includes the Department of Health and Human Services providing free worker training and updating cybersecurity best practices, Google addressing the second 0-day flaw of 2023, Oracle releasing 433 new security fixes, Cisco addressing severe flaws in Industrial Network Director and Modelling Labs, and much more."

Lazarus Hackers Now Spread Linux Malware Through Deceptive Job Offers

Source: https://cyberintelmag.com/malware-viruses/lazarus-hackers-now-spread-linux-malware-through-deceptive-job-offers/

From the Article: "For the first time, a new Lazarus campaign considered a part of “Operation DreamJob” has been found to target Linux users with malware. The latest supply-chain attack against VoIP operator 3CX was carried out by Lazarus, as confirmed with high confidence by ESET experts who found this new targeting."

Industrial security vendors partner to share intelligence about critical infrastructure threats

Source: https://cyberscoop.com/emerging-threat-open-sharing-industrial-cybersecurity/

From the Article: "Some of the largest operational technology cybersecurity vendors are building an open-sourced, opt-in threat intelligence sharing portal to provide early warnings about threats to 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.

Collaboration between CISA, Cyber Command thwarted dangerous cyberattacks, officials said

Source: https://cyberscoop.com/information-sharing-cisa-cyber-commands-rsa-conference/

From the Article: " Information sharing between U.S. Cyber Command and the Cybersecurity and Infrastructure Security Agency at the Department of Homeland Security stopped several potentially disastrous cyberattacks, including a suspected Iranian attack against American elections."

To combat cybercrime, US law enforcement increasingly prioritizes disruption

Source: https://cyberscoop.com/doj-cybercrime-disruption-ransomware/

From the Article: "When a coalition of international law enforcement agencies earlier this year took down a portion of the infrastructure supporting the Hive ransomware syndicate, top officials at the U.S. Department of Justice knew that no arrests were going to be made."

Experts say Congress should do more to keep data brokers from exposing Americans' private information

Source: https://cyberscoop.com/data-brokers-congress-privacy/

From the Article: "During the House Energy and Commerce Oversight and Investigation Committee hearing, witnesses discussed a wide range of harms posed by the data broker industry including the potential to reveal the private health or sexual histories of individuals, provide foreign powers with sensitive information threatening national security and enable predatory marketers and scammers."

Russia's digital warriors adapt to support the war effort in Ukraine, Google threat researchers say

Source: https://cyberscoop.com/russia-sandworm-ukraine-wagner-youtube/

Link back to Table of Contents

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

From the Article: "Russian and pro-Russian operatives continue to modify their hacking and influence operations aimed at Ukraine to extract intelligence and sway public opinion in favor of the war, Google researchers said in a report released Wednesday. The latest tactics include promoting highly produced YouTube videos as well as more traditional phishing campaigns."

How cyber support to Ukraine can build its democratic future

Source: https://cyberscoop.com/ukraine-cyber-aid-russia-war/

From the Article: "In the year since Russia tried and failed to topple Kyiv, Ukraine has repelled the ensuing onslaught of cyber aggression and propaganda more soundly than anyone predicted."

Cyber security technology integration, intrapreneurship & beyond

Source: https://www.cybertalk.org/2023/04/24/cyber-security-technology-integration-intrapreneurship-and-beyond/

From the Article: "A commercial architect will provide structural consulting for a commercial building (or it could be a home, a church…etc.). They are given parameters for the site where the building will be created and there are always certain constraints."

Greening your security: Earth Day tips for cyber security experts

Source: https://www.cybertalk.org/2023/04/21/greening-your-security-earth-day-tips-for-cyber-security-experts/

From the Article: "In considering the environmental impact of security-related initiatives, cyber security professionals can not only contribute to a more sustainable future, but also enhance the overall security and resilience of their organizations."

Vehicles Stolen Using High-Tech Methods by Criminals

Source: https://www.cysecurity.news/2023/04/vehicles-stolen-using-high-tech-methods.html

Link back to Table of Contents

From the Article: "Over the past 20 years, the number of cars stolen in the United States has been reduced by half. However, authorities are now seeing an increasing number of break-ins associated with high-tech techniques being used in these break-ins."

This Evil Extractor Malware Steals Data from Windows Devices

Source: https://www.cysecurity.news/2023/04/this-evil-extractor-malware-steals-data.html

From the Article: "Experts have discovered a hazardous new malware strain that is circulating the internet, stealing sensitive data from victims and, in some cases, installing ransomware as well. The malware, dubbed Evil Extractor, was found by Fortinet cybersecurity experts, who published their findings in a blog post, noting that it was produced and disseminated by a business called Kodex and was marketed as a "educational tool."
"

The IRS is Deploying Four Investigators Across the Globe to Combat Cybercrime

Source: https://www.cysecurity.news/2023/04/the-irs-is-deploying-four-investigators.html

From the Article: "Starting this summer, the Internal Revenue Service (IRS) intends to dispatch four cybercrime investigators to Australia, Singapore, Colombia, and Germany. These four new jobs indicate a major boost in the IRS's global efforts to combat cybercrime, such as cryptocurrency, decentralized finance, and bitcoin laundering services. "

Arizona Teachers' Sensitive Data Stolen in Ransomware Attack on TUSD

Source: https://www.cysecurity.news/2023/04/arizona-teachers-sensitive-data-stolen.html

From the Article: "Hackers have targeted the Tucson Unified School District (TUSD) in Arizona, stealing the social security numbers of 16,000 teachers in a ransomware attack. This incident highlights the continued threat of cybercrime and the vulnerabilities that educational institutions face in terms of data protection."

Link back to Table of Contents

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

Google Workspace Extends Enterprise-Grade Security and Device Management for Hybrid Work With Okta and VMware

Source: https://www.darkreading.com/remote-workforce/google-workspace-extends-enterprise-grade-security-and-device-management-for-hybrid-work-with-okta-and-vmware

From the Article: "JumpCloud integrates with Google Workspace to extend enterprise-quality security capabilities to small and midsize organizations."

Qwiet AI Builds a Neural Net to Catch Coding Vulnerabilities

Source: https://www.darkreading.com/dr-tech/qwiet-ai-builds-a-neural-net-to-catch-coding-vulnerabilities

From the Article: "Code property graphs and a threat feed powered by artificial narrow intelligence help developers incorporate AppSec into DevOps."

Cybersecurity Survival: Hide From Adversarial AI

Source: https://www.darkreading.com/vulnerabilities-threats/cybersecurity-survival-hide-from-adversarial-ai

From the Article: "Consider adding some security-through-obscurity tactics to your organization's protection arsenal to boost protection. Mask your attack surface behind additional zero-trust layers to remove AI's predictive advantage."

Palo Alto Networks Takes Aim At Cyberattacks With the Expansion of Unit 42's Digital Forensics & Incident Response Service Globally

Source: https://www.darkreading.com/operations/palo-alto-networks-takes-aim-at-cyber-attacks-with-the-expansion-of-unit-42-s-digital-forensics-incident-response-service-globally

From the Article: "With 60% of organizations taking more than four days to resolve cybersecurity issues, Unit 42’s Global Incident Response Service dramatically reduces time to remediate threats."

Link back to Table of Contents

The articles have been 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 Policy Group Wants to Improve Cybersecurity Disclosure, Support Researchers

Source: https://www.darkreading.com/edge-articles/new-policy-group-wants-to-improve-cybersecurity-disclosure-support-researchers

From the Article: "The new Security Legal Research Fund and Hacking Policy Council are aimed at protecting "good faith" security researchers from legal threats and giving them a voice in policy discussions."

Labour glitch put voting intentions data of millions at risk

Source: https://www.theguardian.com/politics/2023/apr/16/labour-glitch-put-voting-intentions-data-of-millions-at-risk

From the Article: "The voting intentions of millions of Britons in local authority wards across the country could have been at risk of misuse as a result of a glitch in the Labour party’s main phone-banking system, the Guardian understands."

Fortinet Survey Reveals a Disconnect Between Ransomware Preparedness and Prevention

Source: https://www.fortinet.com/blog/industry-trends/ransomware-protection-survey-for-organizational-prevention

From the Article: "Key findings from the Fortinet 2023 Global Ransomware Report, group think about countermeasures and insight about ransomware campaigns."

How Network Detection and Response Addresses 5 Critical Security Challenges

Source: https://www.fortinet.com/blog/business-and-technology/addressing-security-challenges-with-network-detection-and-response

From the Article: "Read about a few challenges security operation teams face along with areas of consideration for a successful NDR deployment."

Microsoft Changed the Method of Naming the Hacker Groups

Link back to Table of Contents

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

Source: https://gbhackers.com/microsoft-changed-taxonomy/

From the Article: "Microsoft has initiated the naming taxonomy for threat actor groups. Over the years, threat actors have evolved massively, leading to confusion about which threat actor was responsible for which threat activity. "

Enterprise-Attacking Malware Toolkit Analyzing 70 Billion DNS Queries Daily

Source: https://gbhackers.com/enterprise-attacking-malware/

From the Article: "The 'Decoy Dog' malware toolkit, aimed at enterprises, was uncovered recently by the security analysts at Infoblox by analyzing 70 billion DNS records and traffic that differs from typical online behavior."

European Data Protection Board Creates Task Force to Investigate ChatGPT

Source: https://gbhackers.com/task-force-chatgpt/

From the Article: "On Thursday, the European Data Protection Board (EDPB)announced that it had established a task force on ChatGPT, a potentially significant first step towards a uniform policy on setting privacy regulations for artificial intelligence."

MEO - 8,227 breached accounts

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

From the Article: "In early 2023, a corpus of data sourced from the New Zealand based face mask company MEO was discovered. Dating back to December 2020, the data contained over 8k customer records including names, addresses, phone numbers and passwords stored as MD5 Wordpress hashes. MEO did not respond to multiple attempts to report the breach."

Most Common Connected Devices That Pose Risk to Hospitals

Source: https://www.bankinfosecurity.com/armis-device-study-a-21844

Link back to Table of Contents

From the Article: "Nurse call systems present a top cybersecurity risk in clinical environments, but so do an array of other similarly connected nonmedical devices commonly found in healthcare settings, says a new research study by security vendor Armis."

DNS Layer Security Explained. How It Stops Ransomware and Other Cyberattacks

Source: https://heimdalsecurity.com/blog/dns-layer-security/

From the Article: "DNS-Layer Security protects users from threats that arise from inbound and outbound traffic. It refers to monitoring communications between endpoints and the internet at a DNS-layer level. "

SECURITY ALERT: Heimdal® Detects Massive MitID Smishing Campaign Targeting Nordea Bank Customers

Source: https://heimdalsecurity.com/blog/mitid-smishing-nordea-bank/

From the Article: "On the 20th of April, Heimdal®'s SOC team has discovered that an unknown APT has been launching smishing attacks against Nordea Bank customers. "

Attackers are logging in instead of breaking in

Source: https://www.helpnetsecurity.com/2023/04/25/attacks-dwell-time/

From the Article: "Cyberattackers leveraged more than 500 unique tools and tactics in 2022, according to Sophos. The data, analyzed from more than 150 Sophos Incident Response (IR) cases, identified more than 500 unique tools and techniques, including 118 "Living off the Land" binaries (LOLBins)."

AI tools help attackers develop sophisticated phishing campaigns

Source: https://www.helpnetsecurity.com/2023/04/25/ai-phishing-campaigns/

From the Article: "Phishing scams are a growing threat, and cybercriminals' methods are becoming increasingly sophisticated, making them harder to detect and block, according to Zscaler report."

Link back to Table of Contents

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

SentinelOne unveils cybersecurity AI platform

Source: https://www.helpnetsecurity.com/2023/04/25/sentinelone-ai-platform/

From the Article: "Cybercriminals around the world are using generative artificial intelligence (AI) to execute malicious attacks that can take down companies and governments. SentinelOne plans to use the same technologies to defeat them."

Akamai Brand Protector defends against phishing attacks and fake websites

Source: https://www.helpnetsecurity.com/2023/04/24/akamai-brand-protector/

From the Article: "At RSA Conference 2023, Akamai Technologies unveiled Brand Protector, a new solution that detects and disrupts phishing sites, fake stores, and brand impersonations."

Trellix Threat Intelligence enhancements accelerate threat analysis and response

Source: https://www.helpnetsecurity.com/2023/04/24/trellix-threat-intelligence-portfolio/

From the Article: "At RSA Conference 2023, Trellix announced it has expanded its Threat Intelligence portfolio to increase threat expertise and actionable intelligence to help global customers stay ahead of cyber adversaries."

Resecurity to showcase innovative cybersecurity solutions at RSA Conference 2023

Source: https://www.helpnetsecurity.com/2023/04/24/resecurity-solutions-rsa-conference-2023/

From the Article: "Resecurity is excited to announce its participation at RSA Conference 2023, the cybersecurity event that brings together industry leaders and professionals to share knowledge and insights on the latest trends, threats, and solutions."

Study of past cyber attacks can improve organizations' defense strategies

Link back to Table of Contents

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

Source: https://www.helpnetsecurity.com/2023/04/24/cybercriminals-attack-surface/

From the Article: "Ransomware operators have been increasingly launching frequent attacks, demanding higher ransoms, and publicly exposing victims, leading to the emergence of an ecosystem that involves access brokers, ransomware service providers, insurance providers, and ransom negotiators, according to Deepwatch."

Expel Vulnerability Prioritization identifies critical and damaging vulnerabilities

Source: https://www.helpnetsecurity.com/2023/04/24/expel-vulnerability-prioritization-identifies-critical-and-damaging-vulnerabilities/

From the Article: "Expel has released Expel Vulnerability Prioritization, a new solution that highlights which vulnerabilities pose the greatest risk, so organizations can take immediate, informed action."

Onapsis updates its platform to strenghten ERP cybersecurity

Source: https://www.helpnetsecurity.com/2023/04/22/onapsis-platform-update/

From the Article: "Onapsis has unveiled a series of new product updates for the Onapsis Platform. Enriched with the threat intelligence, the Onapsis Platform further simplifies business application security for CISOs and CIOs alike with a new Security Advisor, new updates to its Comply product line, and critical enhancements that streamline code security from application development to production."

Armorblox releases Graymail and Recon Attack Protection to stop malicious emails

Source: https://www.helpnetsecurity.com/2023/04/21/armorblox-graymail-recon-attack-protection/

From the Article: "Armorblox has released its newest product, Graymail and Recon Attack Protection, developed to decrease the time security teams spend managing graymail and mitigate the security risks from malicious recon attacks."

The K-12 Report: A Cybersecurity Assessment of the 2021-2022 School Year

Link back to Table of Contents

Source: https://www.tripwire.com/state-of-security/k-12-report-cybersecurity-assessment

From the Article: "The K-12 Report breaks down the cyber risks faced by public schools across the country and is sponsored by the CIS (Center for Internet Security) and the MS-ISAC (Multi-State Information Sharing & Analysis Center)."

OT-centric, open-source ETHOS platform launched for sharing anonymous early warning threat information

Source: https://industrialcyber.co/vendor/ot-centric-open-source-ethos-platform-launched-for-sharing-anonymous-early-warning-threat-information/

From the Article: " OT cybersecurity companies unveiled Monday plans for ETHOS (Emerging THreat Open Sharing), an open-source, vendor-agnostic technology platform for sharing anonymous early warning threat information across industries with peers and governments."

DHS QHSR document assesses prevailing threats and challenges, as more work needs to be done

Source: https://industrialcyber.co/cisa/dhs-qhsr-document-assesses-prevailing-threats-and-challenges-as-more-work-needs-to-be-done/

From the Article: "The U.S. Department of Homeland Security (DHS) released the latest version of its Quadrennial Homeland Security Review (QHSR) document, which is updated every four years as required by law. The document comes at a time when cyber threats have evolved and increased since the founding of the department. It also informs existing departmental processes for translating priorities into resources, including the DHS Strategic Plan and the annual budget development process."

Eliminating content-borne threats to industrial enterprises

Source: https://industrialcyber.co/interview/eliminating-content-borne-threats-to-industrial-enterprises/

From the Article: "With increased digital connectivity providing a wider canvas to cyber adversaries, organizations, particularly across the industrial and critical infrastructure sectors, are faced with rising instances of malware attacks that continue to rise."

Link back to Table of Contents

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

GAO finds DHS cybersecurity policy needs clarification, as CRRM requirement remains unclear

Source: https://industrialcyber.co/reports/gao-finds-dhs-cybersecurity-policy-needs-clarification-as-crrm-requirement-remains-unclear/

From the Article: "The U.S. Government Accountability Office (GAO) found that selected Department of Homeland Security (DHS) programs have not prepared cybersecurity memorandums ahead of acquisition decision events."

FERC authorizes incentive rate treatment for cybersecurity investments

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. "

US, UK security agencies warn of APT28 hackers exploiting known Cisco vulnerability, issue mitigation action

Source: https://industrialcyber.co/cisa/us-uk-security-agencies-warn-of-apt28-hackers-exploiting-known-cisco-vulnerability-issue-mitigation-action/

From the Article: "Lead security agencies in the U.S. and U.K. published Tuesday a joint Cybersecurity Advisory (CSA) report on the tactics, techniques, and procedures (TTPs) associated with APT28’s exploitation of Cisco routers. The agencies assess that the APT28 group exploits a known vulnerability to carry out reconnaissance of routers and deploy malware, while also accessing poorly maintained Cisco routers and deploying malware on unpatched devices using CVE-2017-6742."

KuCoin Twitter Account Hacked, Losses $22.6K In Crypto Scam

Source: https://informationsecuritybuzz.com/kucoin-twitter-account-hacked-losses-crypto-scam/

Link back to Table of Contents

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

From the Article: "A fake giveaway fraud that resulted in the theft of more than $22.6K in cryptocurrency was promoted by attackers after their access to KuCoin’s Twitter account was compromised. "

Researchers Find 250 Million Artifacts Exposed in Misconfigured Registries

Source: https://www.infosecurity-magazine.com/news/250-million-artifacts-exposed/

From the Article: "More than 65,000 container images also at risk."

US Navy Contractor Fincantieri Marine Group Hit by Cyber-attack

Source: https://www.infosecurity-magazine.com/news/us-navy-contractor-cyberattack/

From the Article: "Shipbuilder said the incident affected its email server and some network operations."

American Bar Association Breach Hits 1.5 Million Members

Source: https://www.infosecurity-magazine.com/news/american-bar-association-breach-1/

From the Article: "Website usernames and passwords stolen in March raid."

CyberSmart makes waves in SME cybersecurity market

Source: https://www.itsecurityguru.org/2023/04/24/cybersmart-makes-waves-in-sme-cybersecurity-market/

From the Article: "CyberSmart recently announced a record year of growth, marked by a large funding round, headcount and customer growth as well as geographical market expansion."

CyberheistNews Vol 13 #17 [Head Start] Effective Methods How To Teach Social

Link back to Table of Contents

Engineering to an AI

Source: https://blog.knowbe4.com/cyberheistnews-vol-13-17-head-start-effective-methods-how-to-teach-social-engineering-to-an-ai

From the Article: "Remember The Sims? Well Stanford created a small virtual world with 25 ChatGPT-powered "people." The simulation ran for 2 days and showed that AI-powered bots can interact in a very human-like way."

Silicon Lifecycle Management Advances With Unified Analytics

Source: https://semiengineering.com/silicon-lifecycle-management-advances-with-unified-analytics/

From the Article: "Integrating data from design through manufacturing in a single platform."

Chip Industry's Technical Paper Roundup: Apr. 25

Source: https://semiengineering.com/chip-industrys-technical-paper-roundup-apr-25/

From the Article: "Quantum light source goes fully on-chip; neuromorphic computing based on SNNs; RISC-V GPUs; data-centric parallelism & chiplets; rowhammer latest; hyperscale HW; graphene; CAN bus security; critical dimension small angle x-ray scattering."

State of the Art And Future Directions of Rowhammer (ETH Zurich)

Source: https://semiengineering.com/state-of-the-art-and-future-directions-of-rowhammer-eth-zurich/

From the Article: "A new technical paper titled “Fundamentally Understanding and Solving RowHammer” was published by researchers at ETH Zurich."

CAN Bus Security Using TDCs (ETH Zurich & CISPA Helmholtz Center)

Source: https://semiengineering.com/can-bus-security-using-tdcs-eth-zurich-cispa-helmholtz-center/

From the Article: "A technical paper titled “EdgeTDC: On the Security of Time Difference of Arrival Measurements in CAN Bus Systems” was published by researchers at ETH Zurich and CISPA Helmholtz Center for Information Security."

Evolving Threats Require New Approaches to Defending Installations

Source: https://www.nationaldefensemagazine.org/articles/2023/4/21/evolving-threats-require-new-approaches-to-defending-installations

From the Article: "“We really don't have any technical gaps per se,” he said. “The technology that I want to improve on — these joint operations — is to speed up the process as well as harden it from cyber and electronic attack, as well as allow for greater volume..”

EMERGING TECHNOLOGY HORIZONS: Condition-Based Maintenance Requires Data Sharing

Source: https://www.nationaldefensemagazine.org/articles/2023/4/19/condition-based-maintenance-requires-data-sharing

From the Article: "What can be done to take the Defense Department’s efforts in predictive maintenance — also known as condition-based maintenance — to the next level?”

Army warns it could lose $5.3 billion if Congress fails to pass budget

Source: https://www.defensenews.com/land/2023/04/19/army-warns-it-could-lose-53-billion-if-congress-fails-to-pass-budget/

From the Article: "WASHINGTON — The U.S. Army will not be able to put $5.3 billion toward modernization efforts key to competing with China if Congress doesn’t pass a budget this year, the service secretary said in a Wednesday House Armed Services Committee hearing."

Let Me Start Weapons R&D Faster, Air Force Secretary Asks Congress

Source: https://www.defenseone.com/policy/2023/04/let-me-start-weapons-rd-faster-air-force-secretary-asks-congress/385388/

From the Article: "Frank Kendall wants freedom from rules that require lawmakers' approval to get anti-China weapons off the ground."

In China's shadow, new Australian defense review focuses on denial, long-range weapons

Source: https://breakingdefense.com/2023/04/in-chinas-shadow-new-australian-defense-review-focuses-on-denial-long-range-weapons/

From the Article: "The review also takes Australia's acquisition strategy to task, saying it's too slow to get capabilities into the hands of the armed forces."

CyberheistNews Vol 13 #16 [Finger on the Pulse]: How Phishers Leverage Recent AI Buzz

Source: https://blog.knowbe4.com/cyberheistnews-vol-13-16-finger-on-the-pulse-how-phishers-leverage-recent-ai-buzz

From the Article: "Curiosity leads people to suspend their better judgment as a new campaign of credential theft exploits a person's excitement about the newest AI systems not yet available to the general public. On Tuesday morning, April 11th, Veriti explained that several unknown actors are making false Facebook ads which advertise a free download of AIs like ChatGPT and Google Bard."

The dark side of budgeting apps: potential security risks

Source: https://latesthackingnews.com/2023/04/25/the-dark-side-of-budgeting-apps-potential-security-risks/

From the Article: "But what if we told you that using a budgeting app could come with security risks too? In this blog post, we'll be exploring how some popular budgeting applications pose potential threats to users' data and how these can be minimized."

Hackers Abuse Outdated Eval PHP WordPress Plugin To Deploy Backdoors

Source: https://latesthackingnews.com/2023/04/24/hackers-abuse-outdated-eval-php-wordpress-plugin-to-deploy-backdoors/

From the Article: "As explained (and as evident from the plugin's official page), Eval PHP received its last major update 11 years ago. The plugin seemed to facilitate WordPress admins in adding PHP codes to an article or blog, disabling PHP error messages, and performing other related functionalities. With time, the plugin stopped receiving updates from its developer, eventually remaining as an abandoned plugin in the WordPress repository."

Lockbit Ransomware Aims To Target macOS Systems – But May Not Be As Successful

Source: https://latesthackingnews.com/2023/04/24/lockbit-ransomware-aims-to-target-macos-systems-but-may-not-be-as-successful/

From the Article: "In a recent tweet, the MalwareHunterTeam disclosed encountering a new LockBit ransomware variant. Identified as "locker_Apple_M1_64" by the researchers, the new malware seems the first such attempt to target Mac specifically."

Service Location Protocol (SLP) Reflection/Amplification Attack Mitigation Recommendations

Source: https://www.netscout.com/blog/asert/slp-reflectionamplification-ddos-attack-vector/

From the Article: "With the computing power and internet transit capacity available to a substantial proportion of abusable SLP reflectors/amplifiers, attackers can potentially launch extremely high-volume, high-impact SLP reflection/amplification DDoS attacks. SLP reflection/amplification can be leveraged in carpet-bombing DDoS attacks targeting one or more entire network address ranges."

Federal Law Enforcement's New Focus is on 'Disruption' of Cybercrime

Source: https://www.nextgov.com/cybersecurity/2023/04/federal-law-enforcements-new-focus-disruption-cybercrime/385597/

From the Article: "Deputy Attorney General Lisa Monaco noted that success will be seen with a "bias towards action," rather than just courtroom victories."

Link back to Table of Contents

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

Eight Years Since The Obama-Xi Agreement, Chinese Hacking Is Worse Than Ever

Source: https://www.scmagazine.com/news/threat-intelligence/eight-years-obama-xi-agreement-chinese-hacking-iworse-than-ever

From the Article: " Eight years ago, the United States and China reached an historic treaty agreement that was designed, in part, to end a persistent deluge of cyberattacks targeting American businesses to steal their corporate secrets and intellectual property.”

Qualys Launches Inaugural Cyber Risk Summit to Share Expert Insights

Source: https://blog.qualys.com/qualys-insights/2023/04/24/qualys-launches-inaugural-cyber-risk-summit-to-share-expert-insights

From the Article: "Cybersecurity professionals from all over are making their way to RSA’s annual conference this week in search of inspiration and expert advice on bolstering their security postures. But for those who could not disrupt their schedules to make the trip, Qualys is providing IT and security practitioners with an easy way to hear fresh perspectives on transformative topics. "

Ransomware threat decreasing but concerns increase over quantum computing-based risks

Source: https://www.continuitycentral.com/index.php/news/technology/8443-ransomware-threat-decreasing-but-concerns-increase-over-quantum-computing-based-risks-2023-thales-data-threat-report

From the Article: "The 2023 Thales Data Threat Report has been released, providing an annual report on the latest data security threats, trends and emerging topics based on a survey of nearly 3000 IT and security professionals in 18 countries."

5 cybercriminal gangs targeting hospitals

Source: https://www.beckershospitalreview.com/cybersecurity/5-cybercriminal-gangs-targeting-hospitals.html

From the Article: "The Health Sector Cybersecurity Coordination Center (HC3) issued a

Link back to Table of Contents

new warning concerning the pro-Russian hacktivist group KillNet."

Rubrik Ups the Ante with $10 Million Ransomware Recovery Warranty - PRWire

Source: https://prwire.com.au/pr/108217/rubrik-ups-the-ante-with-10-million-ransomware-recovery-warranty

From the Article: "First in the cybersecurity industry to offer a ransomware recovery warranty of its kind for qualified customers, Rubrik, the Zero Trust Data Security™ Company, today announced it has increased its Ransomware Recovery Warranty offering from up to $5 million to up to $10 million for recovery-related costs."

Kaspersky finds Nokoyawa ransomware used Windows zero day vulnerability

Source: https://backendnews.net/kaspersky-finds-nokoyawa-ransomware-used-windows-zero-day-vulnerability/

From the Article: "Kaspersky found that a cybercriminal group used a vulnerability in an attempt to deploy Nokoyawa ransomware on Windows OS. The cybersecurity company discovered the zero-day vulnerability in the Microsoft Common Log File System (CLFS) in February."

North Korea's new ransomware targets are healthcare providers - Tech Monitor

Source: https://techmonitor.ai/focus/healthcare-ransomware-north-korea

From the Article: " According to a cybersecurity advisory released by the US government in February, the Democratic People's Republic of Korea (DPRK) has directed its army of elite hackers to create new revenue streams for the regime by infecting healthcare providers with ransomware."

The Evolution of Ransomware and the Best Role of ThreatHunter.ai in Combatting Cyber Attacks -

Source: https://ventsmagazine.com/2023/04/25/the-evolution-of-ransomware-and-the-best-role-of-threathunter-ai-in-combatting-cyber-attacks/

Link back to Table of Contents

From the Article: "As the world continues to become increasingly digitized, the importance of cybersecurity cannot be overstated. The ThreatHunter.ai team is an expert in this field, dedicated to protecting businesses from the threat of ransomware attacks. This blog will define ransomware, explain how it works, and discuss notable recent attacks that have impacted businesses and organizations."

Ransomware prolific in first quarter of 2023 – report - SecurityBrief New Zealand

Source: https://securitybrief.co.nz/story/ransomware-prolific-in-first-quarter-of-2023-report

From the Article: "ReliaQuest has just issued its quarterly ransomware review report. The first quarter of 2023 was the most prolific the ReliaQuest Threat Research Team has ever observed in terms of double-extortion ransomware groups. "

Zach Nunn announces bill to protect schools from cyber attacks - KCCI

Source: https://www.kcci.com/article/iowa-zach-nunn-announces-cybersecurity-bill/43700715

From the Article: "Third District Iowa congressman, Republican Zach Nunn, announced a bipartisan measure to bolster cybersecurity at schools on Monday.Nunn made the announcement at the Des Moines Public Schools district office.The bill, known as The Enhancing K-12 Cybersecurity Act, would help schools bolster their cyberinfrastructure. "

International Cooperation Key to Ransomware Fight | Decipher - Duo Security

Source: https://duo.com/decipher/international-cooperation-key-to-ransomware-fight

From the Article: "The fight against ransomware that has been going on for the better part of a decade now in enterprise and public sector networks has gained some quite powerful allies in recent years in the world's most capable intelligence agencies, and their cooperative efforts are beginning to show some results."

The Decline in Ransomware: Does It Actually Increase Risks for Organizations?

Link back to Table of Contents

Source: https://www.darkreading.com/vulnerabilities-threats/the-decline-in-ransomware-does-it-actually-increase-risks-for-organizations-

From the Article: "Rising ransomware activity has dominated cyber conversations for the better part of the past decade. Global retail giants and thousands of educational institutions and healthcare providers have been among those to fall victim to rampant ransomware attacks."

Phishable multi-factor authentication: A matter of national emergency

Source: https://www.innovationnewsnetwork.com/phishable-multi-factor-authentication-matter-national-emergency/32022/

From the Article: "As the threat of ransomware continues to grow and impact companies, public utilities, hospitals and state and local governments, cybersecurity is now an issue of national concern."

Hacker's Playbook Threat Coverage Roundup: April 25, 2023 - Security Boulevard

Source: https://securityboulevard.com/2023/04/hackers-playbook-threat-coverage-roundup-april-25-2023/

From the Article: "In this version of the Hacker’s Playbook Threat Coverage round-up, we are highlighting newly added coverage for several recently discovered or analyzed ransomware and malware variants, including Sabbath ransomware, 3CXDesktopApp vulnerability, amongst others."

The U.S., U.K. and Germany rank top in ransomware attacks | Security Magazine

Source: https://www.securitymagazine.com/articles/99254-the-us-uk-and-germany-rank-top-in-ransomware-attacks

From the Article: "Cyberattacks have increased over the past few years. Ransomware attacks were analyzed in a recent report by Black Kite. The report looked at 2,708 ransomware victims from April 2022 to March 2023."

Black Kite Research: Ransomware Attacks Resurge with Victims Doubling in 2023 -

StreetInsider

Source: https://www.streetinsider.com/Business+Wire/Black+Kite+Research%3A+Ransomware+Attacks+Resurge+with+Victims+Doubling+in+2023/21547424.html

From the Article: "The report provides a comprehensive analysis of 2,708 ransomware victims with detailed insights into attacks from April 2022 to March 2023. The findings reveal a major ransomware resurgence this year, with the number of victims in March nearly double that of last April and 1.6 times higher than the peak month in 2022."

Global Threat Intelligence Report April - BlackBerry

Source: https://www.blackberry.com/us/en/solutions/threat-intelligence/2023/threat-intelligence-report-april

From the Article: "At BlackBerry, we recognize that in today's world, security leaders must expand their focus beyond technologies and their vulnerabilities. To effectively manage risk, security leaders must continually analyze the global threat landscape and understand how business decisions can influence their organization's threat profile."

Why CISOs and legal need to be on the same page when their company is hacked

Source: https://www.scmagazine.com/analysis/compliance/cisos-legal-department-company-hacked

From the Article: "Your budget is never what you think it needs to be, you're often widely viewed within the organization as a cost center and an obstacle, your influence over larger business decisions that impact security is usually limited, and if there is a damaging breach or incident within an organization, the CISO is the first person that executive leadership and the public look to blame."

50 percent of organizations fell victim to ransomware in 2022 - Security Magazine

Source: https://www.securitymagazine.com/articles/99252-50-percent-of-organizations-fell-victim-to-ransomware-in-2022

From the Article: "The threat of ransomware has greatly affected security leaders and how they run their organizations. Fortinet released a recent report analyzing the results of a survey regarding security leaders’ perspectives on ransomware."

SEO Poisoning, Cobalt Strike Abuse, Emotet Continue to Threaten Healthcare Cybersecurity

Source: https://healthitsecurity.com/news/seo-poisoning-cobalt-strike-abuse-emotet-continue-to-threaten-healthcare-cybersecurity

From the Article: "Cyberthreats during this reporting period include data breaches, ransomware attacks, and other sophisticated threats.”."

Cyberattackers Leveraged More Than 500 Unique Tools and - GlobeNewswire

Source: https://www.globenewswire.com/news-release/2023/04/25/2653659/0/en/Cyberattackers-Leveraged-More-Than-500-Unique-Tools-and-Tactics-in-2022-Sophos-Active-Adversary-Report-for-Business-Leaders-Finds.html

From the Article: " Sophos, a global leader in innovating and delivering cybersecurity as a service, today released its Active Adversary Report for Business Leaders, an in-depth look at the changing behaviors and attack techniques that adversaries used in 2022."

Almost three-quarters of cyber attacks involve ransomware | Computer Weekly

Source: https://www.computerweekly.com/news/365535467/Almost-three-quarters-of-cyber-attacks-involve-ransomware

From the Article: "Ransomware continues to be the most common “end game” scenario in a cyber attack, accounting for 68.4% of all incidents to which the Sophos X-Ops incident response (IR) team responded in 2022, according to data drawn from the supplier’s latest Active adversary report for business leaders, an in-depth look at the evolving attack techniques and behaviours of threat actors."

Businesses are getting much better at dealing with ransomware attacks - TechRadar

Source: https://www.techradar.com/news/businesses-are-getting-much-better-at-dealing-with-ransomware-attacks

From the Article: "Businesses are under the impression they're getting better at detecting, stopping, and mitigating ransomware (opens in new tab) incidents. However, the number of successful attacks is still high, as is the number of businesses that ended up paying the ransom demand, new research has warned."

Trigona ransomware is being spread by threat actors using the Mimikatz hacking tool

Source: https://www.bollyinside.com/news/trigona-ransomware-is-being-spread-by-threat-actors-using-the-mimikatz-hacking-tool/

From the Article: "The Unit42 research team at Palo Alto Networks recently found ransomware called Trigona. It attacks Windows in unusual ways and uses the Mimikatz exploitation tool to load, dump, manipulate, and insert credentials before trying to encrypt files."

Cyberthreat grows in Manufacturing - CXOToday.com

Source: https://www.cxotoday.com/news-analysis/cyberthreat-grows-in-manufacturing/

From the Article: "Digital transformation in the manufacturing sector has brought increased efficiencies, growth and profitability. However, in parallel it has also exposed the sector to increased instances of cyber crimes as malicious actors continuously look for vulnerabilities to exploit through an ever growing sophistication in their approaches. "

Gov. Inslee signs bill to protect Washingtonians from cyber-attacks, ransomware - KIRO 7

Source: https://www.kiro7.com/news/local/gov-inslee-signs-bill-protect-washingtonians-cyber-attacks-ransomware/GXMVQZ3RKNHIHPLH5ZNNHSSVNI/

From the Article: "Governor Inslee signed a bill to protect Washingtonians from cyber-attacks and ransomware, on Friday, announced bill sponsor Senator Matt Boehnke in a news release."

LockBit 3.0 Ransomware Targets Fullerton India - Times Now

Source: https://www.timesnownews.com/technology-science/lockbit-3-0-ransomware-targets-fullerton-india-demand-a-staggering-2400-crores-ransom-in-just-5-days-article-99721253

From the Article: "The group claims to have over 600 GB of sensitive data, including loan agreements, account statuses, bank agreements, international transfers, financial documents, and personal customer information."

Despite being prepared, companies still fall victim to ransomware - IT-Online

Source: https://it-online.co.za/2023/04/24/despite-being-prepared-companies-still-fall-victim-to-ransomware/

From the Article: "Although 78% of organisations polled in a Fortiner survey stated they were “very” or “extremely” prepared to mitigate an attack, the survey found 50% fell victim to ransomware in the last year, and almost half were targeted two or more times."

Expert: Risk level of cyber attacks very high - Breaking Latest News

Source: https://www.breakinglatest.news/technology/expert-risk-level-of-cyber-attacks-very-high/

From the Article: "An increase in so-called ransomwareattacks According to Dörr, this can be observed above all in the economy. "

Rubrik: Ransomware Payment Activity on the Rise - Security Boulevard

Source: https://securityboulevard.com/2023/04/rubrik-ransomware-payment-activity-on-the-rise/

From the Article: "A global survey of more than 1,600 IT and security leaders conducted by Wakefield Research on behalf of Rubrik finds nearly three-quarters (72%) of organizations have complied with a ransomware demand despite nearly all of them (99%) having access to backup and recovery tools."

Ransomware Hackers Using AuKill Tool to Disable EDR Software Using BYOVD Attack

Source: https://thehackernews.com/2023/04/ransomware-hackers-using-aukill-tool-to.html

From the Article: "Threat actors are employing a previously undocumented "defense evasion tool" dubbed AuKill that's designed to disable endpoint detection and response (EDR) software by means of a Bring Your Own Vulnerable Driver (BYOVD) attack."

Malware attacks on the rise in higher ed - EdScoop

Source: https://edscoop.com/malware-attacks-rise-higher-education/

From the Article: "The report, published earlier this month, found that while malware attacks rose, ransomware attacks targeting higher education institutions declined 29% last year."

Key U.S. Navy Shipbuilder Hit in Ransomware Attack - 19FortyFive

Source: https://www.19fortyfive.com/2023/04/key-u-s-navy-shipbuilder-hit-in-ransomware-attack/

From the Article: "Earlier this month, the Wisconsin shipyard that builds the United States Navy's Freedom-class Littoral Combat Ship, as well as the Constellation-class guided-missile frigate was targeted in a ransomware attack."

US Navy Contractor Fincantieri Marine Group Hit by Cyber-attack - Infosecurity Magazine

Source: https://www.infosecurity-magazine.com/news/us-navy-contractor-cyberattack/

From the Article: "Fincantieri Marine Group (FMG) acknowledged the incident in a statement to USNI News last week, saying it affected its email server and some network operations."

Iowa congressman aims to beef up school cybersecurity after Des Moines district breach

Source: https://www.desmoinesregister.com/story/news/politics/2023/04/24/after-des-moines-breach-iowa-congressman-wants-school-cyber-protections/70145823007/

Link back to Table of Contents

From the Article: "An Iowa congressman has introduced legislation attempting to stop cyberattacks against schools after a ransomware attack earlier this year shut down the Des Moines district for two days."

San Bernardino County sheriff's office struggling to recover from 'malware' incident

Source: https://therecord.media/san-bernardino-county-sheriffs-department-cyberattack

From the Article: "The San Bernardino County Sheriff's Department is in the process of recovering from a cyberattack involving malware weeks after it began."

Using the iPhone Recovery Key to Lock Owners Out of Their iPhones

Source: https://www.schneier.com/blog/archives/2023/04/using-the-iphone-recovery-key-to-lock-owners-out-of-their-iphones.html

From the Article: "It's actually a complicated crime. The criminal first watches their victim type in their passcode and then grabs their phone out of their hands. In the basic mode of this attack, they have a few hours to use the phone—trying to access bank accounts, etc.—before the owner figures out how to shut the attacker out. With the addition of the recovery key, the attacker can shut the owner out—for a long time."

SLP flaw allows DDoS attacks with an amplification factor as high as 2200 times

Source: https://securityaffairs.com/145295/hacking/slp-flaw-ddos-attacks.html

From the Article: "A high-severity security vulnerability (CVE-2023-29552, CVSS score: 8.6) impacting the Service Location Protocol (SLP) can be exploited by threat actors to conduct powerful volumetric DDoS attacks."

How Cyber Insurance Changed Cybersecurity

Source: https://securityintelligence.com/articles/how-cyber-insurance-changed-cybersecurity/

From the Article: "When cyber insurance first became available in the 1990s, there wasn't much need for it — or at least, so people thought. The internet as we know it today was still in its infancy, and most organizations didn't see the point of cyber insurance. The original policies were to cover liability around software and media concerns. "

US Cyberwarriors Thwarted 2020 Iran Election Hacking Attempt

Source: https://www.securityweek.com/us-cyberwarriors-thwarted-2020-iran-election-hacking-attempt/

From the Article: "Iranian hackers broke into to a system used by a local government to support its election night operations but were kicked out before any attack could be launched, according to U.S. military and cybersecurity officials."

Google Audit Finds Vulnerabilities in Intel TDX

Source: https://www.securityweek.com/google-audit-finds-vulnerabilities-in-intel-tdx/

From the Article: "Over a nine-month audit, Google researchers identified ten security defects in Intel TDX, including nine vulnerabilities addressed with TDX code changes."

Quick Close Tab adware

Source: https://www.2-spyware.com/remove-quick-close-tab-adware.html

From the Article: "Quick Close Tab is a browser extension with questionable functionality and ad spam Quick Close Tab is a deceptive browser extension that claims to provide a useful feature of quickly closing browser tabs, but it actually contains adware."

Tenable Cyber Watch: Dark Web Marketplace Genesis Market Shut Down, How Using ChatGPT Can Breach Data Privacy Rules, and more

Source: https://www.tenable.com/blog/tenable-cyber-watch-dark-web-marketplace-genesis-market-shut-down-how-using-chatgpt-can-breach

From the Article: "This week's edition of the Tenable Cyber Watch unpacks the international sting operation that successfully shut down notorious cybercrime marketplace Genesis Market and explores how using ChatGPT can breach data privacy rules."

Iranian Hackers Launch Sophisticated Attacks Targeting Israel with PowerLess Backdoor

Source: https://thehackernews.com/2023/04/iranian-hackers-launch-sophisticated.html

From the Article: "An Iranian nation-state threat actor has been linked to a new wave of phishing attacks targeting Israel that's designed to deploy an updated version of a backdoor called PowerLess."

Hackers Exploit Outdated WordPress Plugin to Backdoor Thousands of WordPress Sites

Source: https://thehackernews.com/2023/04/hackers-exploit-outdated-wordpress.html

From the Article: "Threat actors have been observed leveraging a legitimate but outdated WordPress plugin to surreptitiously backdoor websites as part of an ongoing campaign, Sucuri revealed in a report published last week."

Russian Hackers Suspected in Ongoing Exploitation of Unpatched PaperCut Servers

Source: https://thehackernews.com/2023/04/russian-hackers-suspected-in-ongoing.html

From the Article: "Print management software provider PaperCut said that it has "evidence to suggest that unpatched servers are being exploited in the wild," citing two vulnerability reports from cybersecurity company Trend Micro."

Google Cloud Introduces Security AI Workbench for Faster Threat Detection and Analysis

Source: https://thehackernews.com/2023/04/google-cloud-introduces-security-ai.html

From the Article: "Google's cloud division is following in the footsteps of Microsoft with the launch of Security AI Workbench that leverages generative AI models to gain better visibility into the threat landscape."

Link back to Table of Contents

Apache Superset: A story of insecure default keys, thousands of vulnerable systems, few paying attention

Source: https://www.theregister.com/2023/04/25/apache_superset_cve/

From the Article: "Apache Superset until earlier this year shipped with an insecure default configuration that miscreants could exploit to login and take over the data visualization application, steal data, and execute malicious code."

The Threat of Clop Ransomware: How to Stay Safe and Secure

Source: https://flashpoint.io/blog/clop-ransomware-threat/

From the Article: "Clop (also known as Cl0p) is an extortionist ransomware-type malware that originated in 2019 and operates on the Ransomware-as-a-Service (RaaS) model. Clop is a variant of the CryptoMix ransomware family and since its release, there have been several improved versions of the malware."

Zero Trust Steps Up To Shut Down Threat Actors

Source: https://threatconnect.com/blog/zero-trust-steps-up-to-shut-down-threat-actors/

From the Article: "Over a decade ago, Forrester Research introduced the concept of zero trust. Today, zero trust is considered one of the leading frameworks to guide information and security architects in the design of robust and resilient information security architectures. This is a very important aspect of zero trust – it’s a framework that influences security architectures and not a singular technology that you buy."

Attack Surface Management Strategies

Source: https://www.trendmicro.com/en_us/ciso/22/d/attack-surface-management.html

From the Article: "As organizations shift to the cloud in droves, their digital attack surface continues to rapidly expand. We explore how proactive cyber risk management can help harden your defenses and reduce the likelihood of an attack or breach."

Guide to Better Threat Detection and Response (XDR)

Link back to Table of Contents

Source: https://www.trendmicro.com/en_us/ciso/22/k/threat-detection-response-guide.html

From the Article: "50% of security teams in a Trend Micro global study said they're overwhelmed by the number of alerts surfaced by disconnected point products and SIEMs. Discover how XDR can enhance threat detection and response to improve a SecOps team's efficiency and outcomes."

EDA Makes A Frenzied Push Into Machine Learning

Source: https://semiengineering.com/eda-makes-a-frenzied-push-into-machine-learning/

From the Article: "All major vendors now incorporate ML in at least some of their tools, with more ambitious goals for AI in the future."

True 3D-IC Problems

Source: https://semiengineering.com/true-3d-ic-problems/

From the Article: "Stacking logic requires solving some hidden issues; concerns about thermal dissipation may be the least of them."

Designing For In-Circuit Monitors

Source: https://semiengineering.com/designing-for-in-circuit-monitors/

From the Article: "Data from sensors is being used to address a wide variety of issues that can crop up at any point in a chip's lifetime."

The Iranian drones deployed by Russia in Ukraine are powered by stolen Western technology, research reveals | CNN

Source: https://www.cnn.com/2023/04/28/world/iran-drones-russia-ukraine-technology-intl-cmd/index.html

From the Article: "New research has revealed the extent to which Iran has built a powerful weapons industry based on Western technology, and how that technology is being used by Russia against Ukrainian cities."

Council Post: How Generative AI Can Be Used In Electronics Manufacturing

Source: https://www.forbes.com/sites/forbestechcouncil/2023/04/26/how-generative-ai-can-be-used-in-electronics-manufacturing/

From the Article: "A natural question is how generative AI can be used for something as different as PCB manufacturing. In this context, the transformative impact of generative AI centers on data."

Bosch to acquire TSI Semiconductors to boost US chip production

Source: https://techcrunch.com/2023/04/26/bosch-to-acquire-tsi-semiconductors-for-1-5b-to-boost-us-chip-production/

From the Article: "Bosch will acquire the assets of U.S. chipmaker TSI Semiconductors to expand its semiconductor business with silicon carbide chips (SiC), the German engineering and technology giant said Wednesday. Bosch also said that following the acquisition, it will invest $1.5 billion over the next few years to upgrade TSI Semiconductors' manufacturing facilities in Roseville, California."

Rapture, a Ransomware Family With Similarities to Paradise

Source: https://www.trendmicro.com/en_us/research/23/d/rapture-a-ransomware-family-with-similarities-to-paradise.html

From the Article: "In March and April 2023, we observed a type of ransomware targeting its victims via a minimalistic approach with tools that leave only a minimal footprint behind. Our findings revealed many of the preparations made by the perpetrators and how quickly they managed to carry out the ransomware attack."

PFAS & Parts Obsolescence: Act Now to Avoid Disruptions

Source: https://www.manufacturing.net/supply-chain/article/22847085/pfas-parts-obsolescence-act-now-to-avoid-disruptions

Link back to Table of Contents

From the Article: "Understanding where "forever chemicals" exist in your products and processes can help address potential supply chain headaches."

Secure-by-Design Is More Than Just a Cybersecurity Risk Problem

Source: https://www.linkedin.com/pulse/secure-by-design-more-than-just-cybersecurity-risk-problem-ron-ross/

From the Article: "Building trustworthy secure systems has a great deal in common with building a house. It starts with a good architectural plan, input from structural engineers, quality products (e.g., lumber, concrete, plumbing and electrical components, roofing materials, doors and windows), skilled tradespeople to carry out the site grading and construction, building inspections at various stages in the construction process, and a construction supervisor to oversee the work."

ATT&CK v13 released, now offers ICS asset refactoring, analytics pseudocode, mobile data sources - Industrial Cyber

Source: https://industrialcyber.co/vulnerabilities/attck-v13-released-now-offers-ics-asset-refactoring-analytics-pseudocode-mobile-data-sources/

From the Article: "MITRE announced Tuesday release of its ATT&CK v13 which will provide analytics pseudocode, mobile-specific data sources, key website updates, ICS asset refactoring, and more cloud and Linux coverage. The biggest changes in ATT&CK v13 are the addition of detailed detection guidance to some Techniques in ATT&CK for Enterprise, mobile data sources, and two new types of changelogs to help identify more precisely what has changed in ATT&CK."

Apple embezzler admits defrauding company of $17M, gets three years [U]

Source: https://9to5mac.com/2023/04/27/apple-embezzler/

From the Article: "An Apple embezzler who was originally estimated to have cost the Cupertino company $10M has now admitted to fraudulently obtaining a total of $17M over a period of seven years. Dhirendra Prasad worked as a buyer in Apple's global supply-chain division, and engaged in a mix of activities in order to steal the money."

Link back to Table of Contents

OT-centric, open-source ETHOS platform launched for sharing anonymous early warning threat information - Industrial Cyber

Source: https://industrialcyber.co/vendor/ot-centric-open-source-ethos-platform-launched-for-sharing-anonymous-early-warning-threat-information/

From the Article: "OT cybersecurity companies unveiled Monday plans for ETHOS (Emerging THreat Open Sharing), an open-source, vendor-agnostic technology platform for sharing anonymous early warning threat information across industries with peers and governments."

The three major public cloud operators use cloud services as the core to help the development of new generative AI applications

Source:
https://www.digitimes.com.tw/tech/rpt/rpt_show.asp?cnlid=3&cat=AIR&v=20230421-115&n=1

From the Article: "ChatGPT has driven the wave of global generative AI (Generative Artificial Intelligence) technology development, and the potential of AI applications has once again attracted global attention. DIGITIMES Research observed that large public cloud operators (hyperscale..."

Don't get in a semiconductor 'doom spiral' – sector will be back with a bang in 2024

Source:
https://www.theregister.com/2023/04/26/semiconductor_slump_worse_than_feared/

From the Article: "The outlook for the global semiconductor sector appears worse than feared, at least for the near future, with analyst Gartner now expecting to see revenue decline by 11.2 percent for 2023. Weakened demand is being compounded by an oversupply driving down chip prices, it said."

CCC Releases Mechanism Design for Improving Hardware Security Workshop Report " CCC Blog

Source: https://cccblog.org/2023/04/11/ccc-releases-mechanism-design-for-improving-hardware-security-workshop-report/

Link back to Table of Contents

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

From the Article: "The Computing Community Consortium (CCC) is pleased to release the Mechanism Design for Improving Hardware Security Workshop Report. On August 24-25, 2022, the CCC held a visioning workshop on Mechanism Design for Improving Hardware Security in Washington, D.C."

Rensselaer Polytechnic Institute and GlobalFoundries Collaborate in Workforce Education Classes

Source: https://news.rpi.edu/content/2023/04/17/rensselaer-polytechnic-institute-and-globalfoundries-collaborate-workforce

From the Article: "Workforce development collaboration helps inspire, prepare students for a career in semiconductors"

New Standards Push Co-Packaged Optics

Source: https://semiengineering.com/new-standards-push-co-packaged-optics/

From the Article: "Speed, density, distance, and heat all need to be considered; pluggables still have a future."

CYBER - Aviation resilience – cybersecurity threat landscape | EASA

Source: https://www.easa.europa.eu/en/research-projects/cyber

From the Article: "The European Commission published the amended Horizon Europe Work Programme 2023-24 on 31 March 2023. The overall driver of Cluster 5 – "Climate, Energy and Mobility" is to accelerate the green and digital transition, and the associated transformation of the economy, industry and society to achieve climate neutrality in Europe by 2050."

DoD Signs New Administrative Arrangement With European Defence Agency

Source: https://www.defense.gov/News/Releases/Release/Article/3373635/dod-signs-new-administrative-arrangement-with-european-defence-agency/

From the Article: "Activities of cooperation: Initial activities include consultations on the impact of EU Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH) regulation; military mobility; supply chain issues; and the impact of climate change on defense. It also allows for U.S. participation in the open session of the European Defence Standardisation Committee."

Army moves forward with streamlining software acquisition | Federal News Network

Source: https://federalnewsnetwork.com/acquisition/2023/04/army-moves-forward-with-streamlining-software-acquisition/

From the Article: "“The objective of the software pathway specifically is to move us away from a linear, waterfall approach to a more integrated and agile modern approach to software, really recognizing that technology development cycles are more accelerated in the software systems than they are in our hardware systems,” Boatner said."

Purdue researchers build transparent conductors without expensive rare-earth indium

Source: https://www.purdue.edu/newsroom/releases/2023/Q2/purdue-researchers-build-transparent-conductors-without-expensive-rare-earth-indium.html

From the Article: "Purdue University patent-pending polymer technology achieves the same results as indium-based conductors at a lower cost"

Nozomi joins Accenture Security, IBM Security, Mandiant on Elite Cyber Defenders Program - Industrial Cyber

Source: https://industrialcyber.co/critical-infrastructure/nozomi-joins-accenture-security-ibm-security-mandiant-on-elite-cyber-defenders-program/

From the Article: "Industrial cybersecurity vendor Nozomi Networks announced Tuesday its new Elite Cyber Defenders Program, with Accenture Security, IBM Security, and Mandiant (now part of Google Cloud) as initial participants."

ChatGPT is Back in Italy After Addressing Data Privacy Concerns

Source: https://thehackernews.com/2023/04/chatgpt-is-back-in-italy-after.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: "OpenAI, the company behind ChatGPT, has officially made a return to Italy after the company met the data protection authority's demands ahead of April 30, 2023, deadline."

There's No Silver Bullet for Cybersecurity

Source: https://hbr.org/2023/04/theres-no-silver-bullet-for-cybersecurity

From the Article: "Governments are incapable of fixing the insecurity of the internet by themselves, and businesses are unlikely to do it until the economic pain of ignoring the insecurity of the internet becomes greater than the profits it can earn from it."

The Electric: Signs of Progress Toward Electric Airliners

Source: https://www.theinformation.com/articles/the-electric-signs-of-progress-toward-electric-airliners

From the Article: "Now the department, with help, is taking on an even more ambitious goal: batteries to power electric airliners. These won't be four-person flying taxis. The aim is a 100-seat electric plane that can fly 700 miles and displace the larger, kerosene-fueled Boeing 737 and Airbus A320 narrow body jets that currently comprise about 80%..."

SIA Welcomes Commerce Department Action to Advance National Semiconductor Technology Center

Source: https://www.semiconductors.org/sia-welcomes-commerce-department-action-to-advance-national-semiconductor-technology-center/

From the Article: "WASHINGTON—April 25, 2023—The Semiconductor Industry Association (SIA) today released the following statement from SIA President and CEO John Neuffer welcoming the Commerce Department's release of a white paper advancing implementation of the National Semiconductor Technology Center (NSTC), an entity established by the CHIPS and Science Act of 2022 to promote semiconductor research and development."

Center for Internet Security, Google Cloud Announce Strategic Alliance

Source: https://www.cisecurity.org/about-us/media/press-release/center-for-internet-security-google-cloud-announce-strategic-alliance

From the Article: "EAST GREENBUSH. N.Y., April 20, 2023 – The Center for Internet Security, Inc. (CIS®) today announced the launch of the CIS & Google Cloud Alliance to help advance security and resilience for the broader technology ecosystem, with an emphasis on the public sector."

CFIA suspends Mercanti Specialty Foods' licence, no recalls made

Source: https://www.chch.com/cfia-suspends-mercanti-specialty-foods-licence-no-recalls-made/

From the Article: "The CFIA says it pulled the licence because of a lapse in “preventative control measures for the traceability of food products, and with respect to preventative control measures for cooling requirements.”"

America needs to sort out its industrial policy confusion

Source: https://thehill.com/opinion/technology/3952425-america-needs-to-sort-out-its-industrial-policy-confusion/

From the Article: "Likewise, the science component of the CHIPS and Science Act was not true industrial policy, it was science policy. The initial Endless Frontier Act, introduced by Sens. Chuck Schumer (D-N.Y.) and Todd Young (R-Ind.), was closer to an industrial policy as it was focused on applied research in key technology areas critical to staying ahead of China."

How Tucker Carlson Helped Turn Americans Against the Military

Source: https://www.defenseone.com/ideas/2023/04/how-tucker-carlson-helped-turn-americans-against-military/385620/

From the Article: "The partisan firebrand told viewers that uniformed leaders were out to weaken the armed forces and the country itself."

The popularity of maturity

Link back to Table of Contents

Source: https://www.asml.com/en/news/stories/2023/the-popularity-of-maturity

From the Article: "When it comes to microchips, mature technology is sometimes better"

TSMC, GF strike new contracts with car vendors

Source: https://www.digitimes.com/news/a20230426PD210/tsmc-honda-automotive-ic-news-must-read.html

From the Article: "TSMC and GlobalFoundries have both struck long-term contracts with car vendors."

Biden Is Setting Up an $11 Billion Chips Network to Bolster US National Security

Source: https://www.bloomberg.com/news/articles/2023-04-25/biden-set-to-launch-11-billion-chips-program-r-d-centerpiece?leadSource=uverify%20wall

From the Article: "Commerce Department taking early steps to set up tech center. Raimondo's goal is to have program operational by end of year."

Coventry University launches fast-track course in driverless vehicle technology in collaboration with HORIBA MIRA

Source: https://www.coventry.ac.uk/business/business-news/coventry-university-launches-fast-track-course-in-driverless-vehicle-technology-in-collaboration-with-horiba-mira/

From the Article: "A new fast-track course developed by Coventry University aims to augment the skills and knowledge required to keep pace with the advances made in driverless vehicle technology."

STMicroelectronics, GlobalFoundries win EU approval for French chip factory

Source: https://www.reuters.com/technology/stmicroelectronics-globalfoundries-win-eu-approval-french-chip-factory-2023-04-28/

From the Article: "BRUSSELS, April 28 (Reuters) - Chipmakers STMicroelectronics and

GlobalFoundries (GFS.O) secured EU approval on Friday to build a chip factory with French state aid in France."

GlobalFoundries overhauls its process owner model to drive transformation

Source: https://www.cio.com/article/474754/globalfoundries-overhauls-its-process-owner-model-to-drive-transformation.html

From the Article: "Now that Clay can see the faster decision-making and increased productivity that has resulted from the GPO model and platform architecture, he has some lessons to share. The first: Transformation is more than software implementation. GlobalFoundries' GPOs are aware that transformation has two elements: digital enablement and business change, which ensure that your operating model is aligned with the business strategy."

U.S. Military R&D Trends for 2023

Source: https://nstxl.org/u-s-military-rd-trends-for-2023/

From the Article: "For a rundown of the key U.S. military R&D trends for 2023, keep reading."

Gina Raimondo: The 100 Most Influential People of 2023

Source: https://time.com/collection/100-most-influential-people-2023/6269845/gina-raimondo/

From the Article: "As Secretary, she is reviving U.S. manufacturing and rebuilding our technological infrastructure. To return the U.S. to being the global leader in microchip production, she deftly shepherded the CHIPS and Science Act through Congress and is building the diverse coalitions needed to supercharge U.S. semiconductor production, fortify supply chains, and strengthen national security."

NASA aims to end a 50-year old ban on supersonic civilian aircraft in the US

Source: https://interestingengineering.com/transportation/nasa-aims-to-end-a-50-year-old-ban-on-supersonic-civilian-aircraft-in-the-us

Link back to Table of Contents

From the Article: "The agency's Quesst mission aims to develop a quieter Mach+ experience, devoid of supersonic booms."

Intel, CrowdStrike and Zscaler Unveil Compatible Solutions for Zero...

Source: https://www.intel.com/content/www/us/en/newsroom/news/intel-crowdstrike-zscaler-approach-zero-trust.html

From the Article: "Companies demonstrate key integration points available today and will build reference architectures based on real-world deployments that span PC to network edge to cloud."

Japan to give up to $1.8B in subsidies for storage battery, chip projects

Source: https://europe.autonews.com/suppliers/japan-will-invest-storage-battery-and-semiconductor-projects

From the Article: "The Japanese government will subsidize eight storage battery-related proposals, including one plan from Honda, and two semiconductor-related projects."

Taking GaN to the Next Level of Scalability - EE Times

Source: https://www.eetimes.com/taking-gan-to-the-next-level-of-scalability/

From the Article: "Part of EE Times' Improving Tech for Power Efficiency Special Report"

China May Lose Access to German Semiconductor Chemicals

Source: https://www.pcmag.com/news/china-may-lose-access-to-german-semiconductor-chemicals

From the Article: "The German government is considering restricting China's access to key chemicals required to manufacture chips."

Link back to Table of Contents

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

UK PM plans to allocate just £1bn to semiconductor industry

Source: https://www.theregister.com/2023/04/27/uk_pm_sunak_to_allocate/

From the Article: "That's right – we're going to hold the world ransom for... ONE BILLION POUNDS!"

TSMC aims to get newest chip technology into cars faster - ET Auto

Source: https://auto.economictimes.indiatimes.com/news/auto-technology/tsmc-aims-to-get-newest-chip-technology-into-cars-faster/99808726

From the Article: "TSMC is the world's biggest contract manufacturer of semiconductors. Many of the automotive industry's biggest chip suppliers such as NXP Semiconductor and STMicroelectronics NV tap TSMC to make their chips."

SMIC-backed Chinese contract chip maker seeks US$1.4 billion in Shanghai IPO

Source: https://www.scmp.com/business/china-business/article/3218409/smic-backed-chinese-contract-chip-maker-seeks-raise-us14-billion-shanghais-star-market

From the Article: "Semiconductor Manufacturing Electronics Shaoxing (SMES) is offering 1.69 billion shares at 5.69 yuan apiece to raise 9.6 billion yuan (US$1.4 billion). SMES, a joint venture between SMIC and the Shaoxing government, makes power semiconductors and sensors, as well as packaging of analogue chips."

SK Hynix, one of the biggest memory chipmakers, reports record quarterly loss as prices slump

Source: https://www.cnbc.com/2023/04/26/sk-hynix-reports-record-quarterly-operating-loss-forecasts-better-outlook.html

From the Article: "The world's second largest memory chipmaker saw a record quarterly operating loss of 3.4 trillion won ($2.54 billion), widening from the 1.9 trillion won operating loss in the fourth quarter of 2022. However, the chipmaker expects market conditions to improve and revenues to rebound in the second half of the 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.

Korea to build $229 bil. mega chip cluster in Seoul metro area by 2042

Source: https://www.koreatimes.co.kr/www/tech/2023/04/129_347185.html

From the Article: "The government will seek 300 trillion won ($229 billion) in investments from the private sector to establish the world's largest high-tech semiconductor cluster in Gyeonggi Province surrounding Seoul by 2042, the trade and land ministries said Wednesday."

Merck to produce gas for semiconductors in the US

Source: https://www.investmentmonitor.ai/news/company-news/merck-to-produce-gas-for-semiconductors-in-the-us/

From the Article: "German conglomerate Merck is to build a new speciality gas plant in Pennsylvania to support the production of semiconductors."

India’s Chip Design Workforce Under Massive AI Threat

Source: https://analyticsindiamag.com/indias-chip-design-workforce-faces-massive-ai-threat/

From the Article: "AI-based tool for FPGA designers showed about 5 times (more in many cases) improvement in the output by senior engineers"

Will Texas be site of $11 billion National Semiconductor Technology Center?

Source: https://www.bizjournals.com/dallas/news/2023/04/24/semiconductor-research-center-ted-cruz.html

From the Article: "U.S. Sen. Ted Cruz in a visit to Dallas renewed his call for Texas to be the site of an $11 billion center aimed at restoring the nation’s leadership in the advanced semiconductor manufacturing industry. Tens of billions of dollars for new facilities to manufacture advanced semiconductors are being invested in Texas — mostly in North Texas and the Austin area.”

VDA: EU Chips Act must promote automotive-related chips

Source: https://evertiq.com/design/53619

From the Article: "Semiconductor demand from the automotive industry is set to triple by 2030. Unless suitable countermeasures are taken, shortages of semiconductors in the automotive industry will lead to a global drop in production of 20% by 2026, says the German Association of the Automotive Industry (VDA)."

Edwards opens new semiconductor manufacturing facility in Chandler

Source: https://ktar.com/story/5487247/edwards-opens-new-semiconductor-manufacturing-facility-in-chandler/

From the Article: "Edwards is part of the Atlas Copco Group and provides vacuum and abatement services for the global semiconductor industry."

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."

Chinese military evolution tests US reshoring and ally-shoring in its Taiwan strategy

Source: https://www.digitimes.com/news/a20230428VL208/china-chip-war-ic-manufacturing-military.html

From the Article: "The US defense industry is attempting to regear itself in preparation for potential large-scale military conflicts, waking up from a post-Cold War investment hiatus during which counterinsurgency missions topped the Pentagon's agenda."

TSMC sees major fabless clients defer 3nm chip rollouts

Source: https://www.digitimes.com/news/a20230427PD213/tsmc-fabless-amd-apple-ic-manufacturing.html

Link back to Table of Contents

From the Article: "TSMC has obtained 3nm chip order commitments from vendors including AMD, MediaTek, Nvidia, and Qualcomm, which are all looking to defer the delivery of their 3nm generation devices, according to industry sources."

South Korea will offer

Source: https://www.digitimes.com/news/a20230428VL202/south-korea-tesla-battery-gigafactory.html&chid=10

From the Article: "South Korean president Yoon Suk Yeol met with Elon Musk on April 26,asking the Tesla CEO to build a gigafactory in the country. Yoon said South Korea will provide support for location and taxes if the EV company makes the investment."

India smartphone market saw record 1Q decline, iPhone grew by 50% annually

Source: https://www.digitimes.com/news/a20230428VL200/india-smartphone-iphone.html

From the Article: "India's smartphone market experienced a record decline in the first quarter due to weak demand and high inventory. iPhone constituted a 6% market share, with Xiaomi suffering a 44% annual shipment drop."

Chinese firms keen to acquire smaller Korean IC designers to sidestep US curbs

Source: https://www.digitimes.com/news/a20230427PD201/china-acquisition-south-korea-ai-chips-ic-design-distribution.html

From the Article: "Chinese companies and funds reportedly have become keen to acquire or invest in small- and medium-size IC design houses in South Korea, or directly set up R&D branch offices there, seeking to use South Korea as a semiconductor transshipment base..."

Intel foundry business continues to fall, to make Arm SoC on Intel 18A

Source: https://www.digitimes.com/news/a20230428VL201/intel-foundry-chips+components.html

Link back to Table of Contents

From the Article: "Amid a PC slump, Intel posted a sharp fall in sales and profit as the chip giant is hopeful that the worst is over. Intel also confirmed the roadmap for five nodes is on track."

Peru sees lithium mining opportunity in Chile's statist plan

Source: https://www.digitimes.com/news/a20230428VL206/green-energy-lithium-mining-peru.html

From the Article: "Peru is taking a more active role in trying to lure lithium mining investments in light of Chile's decision to take state control of all new projects of the battery metal, an official said."

Chinese truckmaker to boost Mexico presence with eye on US market

Source: https://www.digitimes.com/news/a20230428VL205/china-battery+green-energy-mexico-us-market.html&chid=10

From the Article: "Chinese truckmaker Beiqi Foton Motor Co. is planning a second plant in Mexico to manufacture electric vehicles with an eye on US exports."

Gus Technology not letting China, Japan, and Korea get ahead by building Taiwan's first GWh battery cell factory

Source: https://www.digitimes.com/news/a20230427PD204/battery-cell-gus-technology.html

From the Article: "In the face of a global energy transformation trend, the importance of the battery industry is growing every day. More and more countries are treating the sector as a national strategic industry, hoping to build their own battery supply ecosystem through..."

JCET gearing up for automotive, chiplet demand boom

Source: https://www.digitimes.com/news/a20230427PD214/chiplet-jcet-osat-packaging.html

Link back to Table of Contents

From the Article: "Jiangsu Changjiang Electronics Technology (JCET), the largest China-based OSAT company, is gearing up for a surge in demand for automotive and chiplet solutions with its expanding system- and wafer-level, and 2.5D/3D advanced packaging technology por..."

Samsung says 1b DRAM production almost ready

Source: https://www.digitimes.com/news/a20230427PD207/dram-memory-chips-must-read-samsung.html

From the Article: "Samsung Electronics has disclosed that preparations for volume production of 1b DRAM (12nm) are approaching the final stages."

TI sees market uncertainties for all applications except automotive

Source: https://www.digitimes.com/news/a20230427PD202/texas-instruments-automotive-industrial-control-ic-design-distribution-tsmc.html

From the Article: "Leading analog IC vendor Texas Instruments (TI) has seen its overall financial results for first-quarter 2023 meet its original financial guidance, but its observation is that macro market environment is still full of uncertainties, with the exception..."

TSMC, UMC step up automotive IC deployment

Source: https://www.digitimes.com/news/a20230426PD216/automotive-ic-tsmc-umc.html

From the Article: "TSMC and United Microelectronics (UMC) have both stepped up their deployments in the automotive IC field."

Statuses of South Korea IC substrate industry

Source: https://www.digitimes.com/news/a20230426RS400.html&chid=2

From the Article: "Supply chain disruptions caused by COVID-19 and increasing demand for advanced packaging processes had put IC substrates in tight supply."

NAND flash beyond 200 layers? Chinese equipment vendor admits difficulty

Source: https://www.digitimes.com/news/a20230425PD207/amec-china-memory-chips-must-read-nand-flash-ymtc.html

From the Article: "As a result of an SCMP report indicating that Chinese memory chip maker Yangtze Memory Technologies Corp. (YMTC) is planning to use domestically sourced equipment to make advanced flash memory products following US sanctions, China's homegrown..."

Different chip segments vary in inventory depletion speed

Source: https://www.digitimes.com/news/a20230424PD201/ic-design-distribution-it-components-peripherals-notebook-shipments.html

From the Article: "Inventory depletion paces vary with different supply chains, with panel, notebook, motherboards and graphic card sectors taking the lead to bottom out while memory and handset IC segments are likely to wait till the fourth quarter of the year, according..."

Marvell demos 3nm data infrastructure silicon

Source: https://www.digitimes.com/news/a20230424VL204/3d-packaging-marvell-tsmc.html

From the Article: "Marvell Technology has demonstrated high-speed, ultra-high bandwidth silicon interconnects manufactured using Taiwan Semiconductor Manufacturing Company's (TSMC) 3-nanometer (3nm) process. Marvell's industry-first silicon building blocks in this node..."

Huawei cuts itself off from reliance on foreign ERP systems

Source: https://www.digitimes.com/news/a20230421VL203/china-huawei-oracle-us-china-trade-war.html

Link back to Table of Contents

From the Article: "After two decades during which Huawei counted on Oracle and its suppliers for software for daily business operations, the
US-sanctioned Chinese company announced it successfully cut itself off its reliance on foreign ERP systems amid China's nationally-mobilized import substitution."

'Smart' military base upgrades delayed - Taipei Times

Source: https://www.taipeitimes.com/News/front/archives/2023/04/30/2003798859

From the Article: "SECURITY: More than half of the 61 sites that should have had monitoring installed to prevent unauthorized access were not upgraded by the end of last year as planned"

The US must do more to support Taiwan: Bolton - Taipei Times

Source: https://www.taipeitimes.com/News/front/archives/2023/04/30/2003798860

From the Article: "TAKE A STAND: China must be made aware that Taiwan will fight, while the US and allied nations must help with preparations, the ex-US security adviser said"

N Korea threatens 'serious danger' over US, S Korea deal - Taipei Times

Source: https://www.taipeitimes.com/News/front/archives/2023/04/30/2003798862

From the Article: "North Korean leader Kim Jong-un's powerful sister, Kim Yo-jong, yesterday said that a US-South Korean agreement aimed at strengthening deterrence against Pyongyang would lead to "more serious danger," state media reported. The US and South Korea this week vowed that North Korea would face a nuclear response and the "end" of the leadership there should it use its own nuclear weapons against the allies, as the two countries' presidents met in Washington."

Sunak, Meloni call for security, calm in Strait - Taipei Times

Source: https://www.taipeitimes.com/News/front/archives/2023/04/29/2003798805

From the Article: "FRENCH COOPERATION: A delegation visited Taipei to demonstrate ‘friendship and respect,’ in one of many meetings of global leaders to occur this week"

Taiwan envoy in France urges European firms to boost cooperation with Taipei - Taipei Times

Source: https://www.taipeitimes.com/News/taiwan/archives/2023/04/30/2003798877

From the Article: "“Half of the world’s containers go through the Taiwan Strait. These would be at risk. So businesses have an interest to help everyone maintain peace,” Wu said. During a separate interview on Bloomberg Television, Wu also pushed for boosting Taiwan’s cooperation on the production of semiconductors, not just with France."

US and South Korea agree to minimize uncertainties on chip subsidy: ministry - Taipei Times

Source: https://www.taipeitimes.com/News/biz/archives/2023/04/29/2003798793

From the Article: "ENTICING INVESTMENT: Seoul’s trade ministry said that the measures would address the concerns of local chipmakers such as Samsung Electronics and SK Hynix"

US chip incentives will not end Asia cost gap: official - Taipei Times

Source: https://www.taipeitimes.com/News/biz/archives/2023/04/29/2003798792

From the Article: "Despite the investment and development incentives that the administration of US President Joe Biden is providing, it would still be cheaper to make chips in Asia — where many customers are based — which could prompt plant closures in a decade, Ferry said. Schmidt said his office is thinking about how to use the US$39 billion as starter capital to create an ecosystem that would have “self-sustaining competitive dynamics.”"

GDP declines 3.02% amid chip slump - Taipei Times

Source: https://www.taipeitimes.com/News/biz/archives/2023/04/29/2003798783

Link back to Table of Contents

The articles have been 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: "SHARPEST DROP SINCE 2009: The decline was more than twice as steep as expected by economists and prompted the DGBAS to slash its full-year growth forecast to 1.67%"

Samsung expects growth despite record chip losses - Taipei Times

Source: https://www.taipeitimes.com/News/biz/archives/2023/04/28/2003798724

From the Article: "RECOVERY: The memorychip industry has likely passed the worst of its weak demand, so the company’s chip division could see growth later this year, a banker said"

Germany eyes limiting chip chemicals to China - Taipei Times

Source: https://www.taipeitimes.com/News/biz/archives/2023/04/28/2003798719

From the Article: "EXPORT RESTRICTIONS? If implemented, German firms such as Merck and BASF would be barred from selling some semiconductor chemicals to Chinese companies"

TSMC on track for 2nm advanced chips by 2025 - Taipei Times

Source: https://www.taipeitimes.com/News/biz/archives/2023/04/28/2003798715

From the Article: "Taiwan Semiconductor Manufacturing Co (TSMC, 台積電) has announced that plans to bring its advanced 2-nanometer (nm) technology into mass production by 2025 are still on track."

China might use AI to sow chaos: NSB - Taipei Times

Source: https://www.taipeitimes.com/News/taiwan/archives/2023/04/27/2003798692

From the Article: "‘HYBRID THREAT’: The development of deepfake technology and ChatGPT, as well as social media, could help the CCP intensify cognitive warfare against Taiwan"

Link back to Table of Contents

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

UMC profit plunges amid low demand - Taipei Times

Source: https://www.taipeitimes.com/News/biz/archives/2023/04/27/2003798655

From the Article: "WEAKEST IN FIVE QUARTERS: Net profit declined 18.3 percent from a year earlier, as an inventory correction continued to weigh on demand, the chipmaker said"

Virginia to open trade office in Taiwan - Taipei Times

Source: https://www.taipeitimes.com/News/front/archives/2023/04/25/2003798563

From the Article: "IMPORTANT PARTNER: Virginia is the biggest exporter to Taiwan among all states in the US, while it imports more than US$1 billion of products from the nation every year"

Chips can be beneficial to Italian diplomacy - Taipei Times

Source: https://www.taipeitimes.com/News/editorials/archives/2023/04/25/2003798558

From the Article: "Italian officials have expressed a wish to increase cooperation with Taiwan on the production and export of semiconductors, Bloomberg reported. The officials also said that Italy might be willing to stop participating in China's Belt and Road Initiative."

TSMC, ARK ink renewable power purchase contract - Taipei Times

Source: https://www.taipeitimes.com/News/biz/archives/2023/04/22/2003798379

From the Article: "Taiwan Semiconductor Manufacturing Co (TSMC, 台積電) yesterday said it has signed a joint procurement contract with ARK Power Co (誠新電力) to provide 20 terawatt-hours of solar energy as part of the chipmaker's broader efforts to reduce its carbon footprint together with companies in its supply chain."

Youngkin seeks chip supply in Japan - Taipei Times

Source: https://www.taipeitimes.com/News/world/archives/2023/04/28/2003798764

Link back to Table of Contents

The articles have been 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: "‘CRITICAL SECTORS’: The Virginia governor said his state is home to 130 Japanese companies and he hoped to forge new partnerships particularly in semiconductors"

Macronix slides into red due to inventory losses - Taipei Times

Source: https://www.taipeitimes.com/News/biz/archives/2023/04/26/2003798603

From the Article: "STOCK UP: Sluggish demand for memory chips used in consumer electronics and PCs led inventory valuation losses to swell more than NT$200 million last quarter"

[ANALYSIS] Is Yoon-Biden summit a win-win for both S. Korea, US?

Source: https://www.koreatimes.co.kr/www/nation/2023/04/120_350013.html

From the Article: "Experts divided over outcomes of summit to mark 70th anniversary of alliance"

Yoon becomes 1st S. Korean to receive briefings at Pentagon, DARPA

Source: https://www.koreatimes.co.kr/www/nation/2023/04/205_349983.html

From the Article: "Yoon, who is on a state visit to the U.S., is the first South Korean president to visit the NMCC and the first foreign leader to visit DARPA. It appears to be a symbolic gesture from the U.S. to show its commitment to the Seoul-Washington alliance. It is also seen as a follow-up measure to the Washington Declaration, which calls for the two countries' leaders to discuss nuclear and strategic planning against North Korea's threats."

Washington agrees to lessen burden on Korean firms investing in US

Source: https://www.koreatimes.co.kr/www/tech/2023/04/129_350008.html

From the Article: "South Korea and the United States have agreed to minimize uncertainty and business burdens for Korean companies investing in the U.S. arising from the implementation of the CHIPS Act, according to the Ministry of Trade, Industry and Energy, Friday. The two nations also decided to work closely with Korean companies to address their concerns regarding the Inflation Reduction Act (IRA)."

Industrial output up 1.6% in March, led by chips

Source: https://www.koreatimes.co.kr/www/biz/2023/04/602_349972.html

From the Article: "The production of semiconductors shot up 35.1 percent from the previous month. The sector's output, however, nevertheless fell 26.8 percent from a year earlier."

Full text of Yoon's address at US Congress

Source: https://www.koreatimes.co.kr/www/nation/2023/04/113_349964.html

From the Article: "The following is South Korean President Yoon Suk Yeol's address to a joint session of U.S. Congress in commemoration of the 70th anniversary of the South Korea-U.S. alliance, delivered Thursday."

KITA chief discusses ways to boost bilateral trade with US politicians

Source: https://www.koreatimes.co.kr/www/tech/2023/04/129_349934.html

From the Article: "In the meeting, they discussed support for semiconductor and electric vehicle (EV) subsidies, and the bill to establish a new visa quota for Korean professional workers. Kim jointly introduced the Partnering with Korea Act with Democratic Rep. Gerry Connolly, which includes issuing 15,000 professional employment visas annually to Koreans in specialized fields."

Text of Joint Statement between US, Korea

Source: https://www.koreatimes.co.kr/www/nation/2023/04/113_349872.html

From the Article: "Together, we will increase our comprehensive global cooperation, deepen our robust regional engagement, and broaden our ironclad bilateral ties during the next 70 years of our alliance to face the 21st century's most difficult challenges head-on."

SK hynix suffers $2.54 bil. loss in Q1 on memory chip bust

Source: http://www.koreatimes.co.kr/www/tech/2023/04/129_349843.html

From the Article: "Chipmaker expects conditions to improve from Q2"

Samsung, SK in dilemma over US pressure not to boost chip output in China

Source: http://www.koreatimes.co.kr/www/tech/2023/04/129_349752.html

From the Article: "Gov't urged to take firm stand on Washington's request"

Korea's Q1 exports sink 12.6% on weak chip demand

Source: http://www.koreatimes.co.kr/www/biz/2023/04/602_349737.html

From the Article: "Korea's exports dipped nearly 13 percent in the first quarter of 2023 due largely to sluggish chip shipments, a trade body said Tuesday."

7 US firms to invest $4.4 bil. in Korea

Source: http://www.koreatimes.co.kr/www/art/2023/04/398_349702.html

From the Article: "During the ceremony, the six companies pledged to make investments totaling $1.9 billion and establish manufacturing facilities related to clean hydrogen, semiconductors and carbon neutrality in Korea. The six are hydrogen companies Air Products and Plug Power, chipmaker On Semiconductor, thermoplastics manufacturer Greene Tweed and eco-friendly technology companies PureCycle Technologies and EMP Belstar."

Samsung faces tough legal battle against Netlist

Source: http://www.koreatimes.co.kr/www/tech/2023/04/129_349662.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: "Samsung Electronics is facing a tough legal battle in the United States as it has been ordered by a jury to pay over $303 million to U.S. memory module company Netlist for infringing five patents."

US urges Korea not to fill chip shortfalls in China if Micron banned: FT

Source: http://www.koreatimes.co.kr/www/world/2023/04/501_349619.html

From the Article: "The United States asked South Korea to urge its chipmakers not to fill any market gap in China if Beijing bans memory chipmaker Micron Technology from selling chips, the Financial Times reported on Sunday."

EU racing to devise new China strategy with 'de-risking' at its core

Source: https://www.scmp.com/news/china/diplomacy/article/3218859/eu-racing-devise-new-china-strategy-de-risking-its-core

From the Article: "Public spats over ways to deal with Beijing and the messaging on Taiwan have injected new sense of urgency into policymaking process. EU members find de-risking more palatable than decoupling, but agreeing on 'the economic stuff' is easier than on political issues, diplomat notes."

US-China relations will ultimately be decided by hard economics

Source: https://www.scmp.com/comment/opinion/article/3218570/us-china-relations-will-ultimately-be-decided-hard-economics

From the Article: "The US economy seems to be heading towards recession, while China's economy appears to be recovering quite well. Washington's recently altered tone in official exchanges with Beijing may reflect this changing reality."

China, Singapore to launch joint military drills as Beijing seeks to counter US

Source: https://www.scmp.com/news/asia/southeast-asia/article/3218122/china-singapore-launch-first-joint-military-drills-2-years-beijing-seeks-counter-us-influence

From the Article: "China's navy plans to deploy a missile-bearing frigate and a

minehunting ship to the joint maritime exercise with Singapore.
The combined drills will be their first since 2021, which followed the upgrade of a bilateral defence pact in 2019 to include bigger-scale exercises."

Chinese envoy warns Tokyo on Taiwan, links Japanese man's detention to spying

Source: https://www.scmp.com/news/china/diplomacy/article/3218864/chinese-envoy-warns-japan-taiwan-red-line-links-japanese-mans-detention-spying

From the Article: "'Harmful' to connect China's internal affairs to Japanese security, ambassador Wu Jianghao says, slamming Tokyo for aligning with the US on Taiwan. Astellas Pharma employee's case not that of an innocent Japanese citizen being taken into custody, Wu says at the Japan National Press Club."

Hong Kong hits out at US over 'Made in China' rule for exports after WTO meeting

Source: https://www.scmp.com/news/hong-kong/politics/article/3218865/hong-kong-hits-out-us-over-made-china-rule-exports-after-meeting-geneva

From the Article: "US undermining integrity of rules-based multilateral trading system embodied by WTO, government spokesman says. WTO in December called for Washington to drop labelling rule, triggering appeal now stuck in limbo after US blocks appointments of judges to panel."

China trade group warns of countermeasures to Japan chip export curbs

Source: https://www.scmp.com/tech/tech-war/article/3218861/tech-war-chinas-chip-trade-group-warns-resolute-countermeasures-over-japans-semiconductor-export

From the Article: "The China Semiconductor Industry Association has called on Tokyo not to 'abuse export control measures' that would damage bilateral cooperation. Japan is slated to require local companies, such as Tokyo Electron, to apply for licences to ship certain advanced chip-making tools to China starting July."

Chinese memory chip suppliers said to benefit from Beijing's probe into Micron

Source: https://www.scmp.com/tech/tech-war/article/3218631/tech-war-beijingscybersecurity-review-us-memory-chip-maker-micron-opens-opportunity-chinese

From the Article: "A possible ban on Micron products in China is expected to see Yangtze Memory Technologies Co and other mainland suppliers fill any void in the market. The local inventory of memory products has not been affected by Beijing’s Micron review owing to an abundant supply from alternative mainland sources."

SMIC-backed Chinese contract chip maker seeks US$1.4 billion in Shanghai IPO

Source: https://www.scmp.com/business/china-business/article/3218409/smic-backed-chinese-contract-chip-maker-seeks-raise-us14-billion-shanghais-star-market

From the Article: "Semiconductor Manufacturing Electronics Shaoxing (SMES) is offering 1.69 billion shares at 5.69 yuan apiece to raise 9.6 billion yuan (US$1.4 billion). SMES, a joint venture between SMIC and the Shaoxing government, makes power semiconductors and sensors, as well as packaging of analogue chips."

Shanghai woos semiconductor and AI projects with generous subsidies

Source: https://www.scmp.com/tech/policy/article/3218324/shanghai-woos-semiconductor-and-ai-projects-generous-subsidies-lining-behind-beijings-innovation

From the Article: "The city authority also plans to boost key AI projects, such as intelligent chips, core algorithms, operating systems and basic software. New policy is aimed at enhancing ‘vitality of industrial development’ and improving ‘city’s core competitiveness’."

US and South Korean leaders set to discuss Taiwan, semiconductors

Source: https://www.scmp.com/news/china/article/3218217/us-south-korea-summit-taiwan-semiconductors-agenda-between-joe-biden-and-yoon-suk-yeol

From the Article: "‘Very robust discussion’ on fraught topics expected for second state visit hosted by Biden administration and first involving an Indo-Pacific leader. Washington seeks ‘a more secure global telecommunications ecosystem and a more resilient supply chain for semiconductors’, says spokesman."

Link back to Table of Contents

China’s chip-focused funds make hefty gains from stock picks amid US sanctions

Source: https://www.scmp.com/business/china-business/article/3218031/tech-war-ex-huawei-manager-turns-sanction-adversity-56-cent-gain-chinas-chip-focused-funds-lure-us29

From the Article: "Lei Tao’s Topsperity Semiconductor Industry fund returned 56 per cent so far this year, while his top five stock picks surged by 35 to 240 per cent. In all, 36 onshore semiconductor-focused equity funds lured 20.2 billion yuan (US$2.9 billion) in fresh inflows last quarter: EastMoney data."

Intel sees ‘green shoots’ in chip market with rebound in second half

Source: https://www.scmp.com/tech/big-tech/article/3218667/intel-sees-green-shoots-chip-market-shares-rally-optimistic-2023-outlook

From the Article: "Intel predicted that gross margins will widen in the second half and expects shipments to reach 270 million units this year. Intel is confronting a massive pile-up of inventory, weak demand and the loss of market share as it tries to speed up the introduction of new technology."

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 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."

New report shows Arizona manufacturing 'renaissance'

Source: https://www.thecentersquare.com/arizona/article_949ba782-e625-11ed-b73b-4f6c6ace8b79.html

From the Article: "A report from the Common Sense Institute, a Phoenix-based conservative think tank, determined that Arizona topped all other states in March for adding 2,000 manufacturing jobs and $77.6 billion in “direct sales and output” from the sector in 2022, which the group said in a roughly 40% uptick since 2017."

Bosch buys US semiconductor foundry to expand EV chip output

Source: https://www.reuters.com/technology/bosch-buys-us-semiconductor-foundry-expand-ev-chip-output-2023-04-26/

From the Article: "DETROIT, April 26 (Reuters) - Germany's Bosch Group has agreed to buy key assets of California chip manufacturer TSI Semiconductors and invest $1.5 billion to expand U.S. production of silicon carbide chips for electric vehicles."

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."

Boosting chip production is "an investment in America's national security," Commerce secretary says

Source: https://www.marketplace.org/2023/04/25/boosting-chip-production-an-investment-in-national-security-commerce-secretary-says/

From the Article: ""Marketplace" host Kai Ryssdal spoke with Raimondo at the Commerce building in Washington, D.C. The following is an edited transcript of their conversation. "

Improving your bottom line with cybersecurity top of mind

Source: https://cybersecurity.att.com/blogs/security-essentials/improving-your-bottom-line-with-cybersecurity-top-of-mind

From the Article: "In times of economic downturn, companies may become reactive in their approach to cybersecurity management, prioritizing staying afloat over investing in proactive cybersecurity measures. However, it's essential to recognize that cybersecurity is a valuable investment in your company's security and stability."

Link back to Table of Contents

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

Supply Chain Weekly Wrap-Up 04/21/2023-04/27/2023

Source: https://www.allthingssupplychain.com/supply-chain-weekly-wrap-up-04-21-2023-04-27-2023/

From the Article: "A report from Bloomberg on Thursday suggested that the German government was considering restrictions on the chemicals in order to reduce Germany's exposure to China. The report suggested the move was in early stages of discussion but officials taking part in the talks were aware that such a step could damage business ties with Beijing."

Anomali Cyber Watch: Two Supply-Chain Attacks Chained Together, Decoy Dog Stealthy DNS Communication, EvilExtractor Exfiltrates to FTP Server

Source: https://www.anomali.com/blog/anomali-cyber-watch-two-supply-chain-attacks-chained-together-decoy-dog-stealthy-dns-communication-evilextractor-exfiltrates-to-ftp-server

From the Article: "The various threat intelligence stories in this iteration of the Anomali Cyber Watch discuss the following topics: APT, Cryptomining, Infostealers, Malvertising, North Korea, Phishing, Ransomware, and Supply-chain attacks."

Malware Analysis Tool: retoolkit

Source: https://www.blackhatethicalhacking.com/tools/retoolkit/

From the Article: "Retoolkit is a Reverse Engineering and Malware Analysis tool developed by the Mentebinaria group. It aims to provide a set of useful utilities for binary analysis and reverse engineering which includes various tools such as disassemblers, debuggers, hex editors, and memory viewers. It supports a wide range of platforms including Windows, Linux, macOS, and even some embedded systems."

Global Cyberattacks Continue to Rise with Africa and APAC Suffering Most

Source: https://blog.checkpoint.com/research/global-cyberattacks-continue-to-rise/

Link back to Table of Contents

The articles have been 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: "Highlights: Global weekly attacks rose by 7% in Q1 2023 versus same quarter last year, , with each organization facing an average of 1248 attacks per week."

When Cyberattacks Have Nothing to Do with You – The Escalation of DDoS Cyberattacks due to Hacktivism

Source: https://blog.checkpoint.com/security/when-cyberattacks-have-nothing-to-do-with-you-the-escalation-of-ddos-cyberattacks-due-to-hacktivism/

From the Article: "Hacktivist attacks have been escalating across the world in recent years with reputed hacktivist groups growing in both size and influence. Last year, a Malaysia-linked hacktivist group attacked targets in India, seemingly in reprisal for a representative of the ruling Bharatiya Janata Party (BJP) making remarks felt to be insulting to the prophet Muhammad."

Threat Source newsletter (April 27, 2023) — New Cisco Secure offerings and extra security from Duo

Source: https://blog.talosintelligence.com/threat-source-newsletter-april-27-2023-new-cisco-secure-offerings-and-extra-security-from-duo/

From the Article: "I'm writing this earlier in the week as I get ready for some personal travel (everyone is lucky I passed on writing another Cybersecurity Mock Draft), so apologies if I miss anything major that happens at RSA."

Quarterly Report: Incident Response Trends in Q1 2023

Source: https://blog.talosintelligence.com/quarterly-report-incident-response-trends-in-q1-2023/

From the Article: "In a novel increase compared to previous quarters, Cisco Talos Incident Response (Talos IR) reports that web shells were the most-observed threat in the first quarter of 2023, comprising nearly a fourth of the incidents Talos IR engaged in. The functionality of these web shells and the specific vulnerabilities and weaknesses in the platforms they targeted varied. "

5 ways threat actors can use ChatGPT to enhance attacks

Source: https://www.csoonline.com/article/3694931/5-ways-threat-actors-can-use-chatgpt-to-enhance-attacks.html

From the Article: "The Cloud Security Alliance (CSA) has revealed five ways malicious actors can use ChatGPT to enhance their attack toolset in a new report exploring the cybersecurity implications of large language models (LLMs). "

AI-powered chatbots: the threats to national security are only beginning

Source: https://www.csoonline.com/article/3694509/ai-powered-chatbots-the-threats-to-national-security-are-only-beginning.html

From the Article: "The United Kingdom’s National Cyber Security Center (NCSC) recently issued a warning to its constituents on the threat posed by artificial intelligence (AI) to the national security of the UK. This was followed shortly by a similar warning from NSA cybersecurity director Rob Joyce. It is clear there is great concern from many nations surrounding the challenges and threats posed by AI."

Cybercrime group FIN7 targets Veeam backup servers

Source: https://www.csoonline.com/article/3694852/cybercrime-group-fin7-targets-veeam-backup-servers.html

From the Article: "Researchers warn that a financially motivated cybercrime group known as FIN7 is compromising Veeam Backup & Replication servers and deploying malware on them. It's not yet clear how attackers are breaking into the servers, but a possibility is that they're taking advantage of a vulnerability patched in the popular enterprise data replication solution last month."

5 most dangerous new attack techniques

Source: https://www.csoonline.com/article/3694892/5-most-dangerous-new-attack-techniques.html

From the Article: "Cyber experts from the SANS Institute have revealed the five most dangerous new attack techniques being used by attackers including cyber criminals and nation-state actors. They were presented in a session at the RSA Conference in San Francisco, where a panel of SANS analysts explored emerging Tactics, Techniques, and Procedures (TTPs) and advised organizations on how to prepare for them."

Link back to Table of Contents

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

Chinese hackers launch Linux variant of PingPull malware

Source: https://www.csoonline.com/article/3694891/chinese-hackers-launch-linux-variant-of-pingpull-malware.html

From the Article: "Chinese state-sponsored threat actor Alloy Taurus has introduced a new variant of PingPull malware, designed to target Linux systems, Palo Alto Networks said in its research. Along with the new variant, another backdoor called Sword2033 was also identified by the researchers."

Why Russia's cyber arms transfers are poor threat predictors

Source: https://www.csoonline.com/article/3694614/why-russias-cyber-arms-transfers-are-poor-threat-predictors.html

From the Article: "The history of international cyber conflict is remarkably long and storied. The timeline of major cyber threat events stretches back nearly four decades, but it is really only the last decade that has seen the widespread proliferation of national cyber forces."

Iranian cyberspies deploy new malware implant on Microsoft Exchange Servers

Source: https://www.csoonline.com/article/3694850/iranian-cyberspies-deploy-new-malware-implant-on-microsoft-exchange-servers.html

From the Article: "A cyberespionage group believed to be associated with the Iranian government has been infecting Microsoft Exchange Servers with a new malware implant dubbed BellaCiao that acts as a dropper for additional payloads. The malware uses DNS queries to receive commands from attackers encoded into IP addresses."

New DDoS amplification vector could enable massive attacks

Source: https://www.csoonline.com/article/3694650/new-ddos-amplification-vector-could-enable-massive-attacks.html

From the Article: "Security researchers sounded the alert about a vulnerability in an

UDP-based network service called the Service Location Protocol (SLP) that can be abused to amplify DDoS attacks."

BrandPost: AT&T Cybersecurity Insights Report

Source: https://www.csoonline.com/article/3685434/atandt-cybersecurity-insights-report.html

From the Article: "This year's Annual AT&T Cybersecurity Insights Report focuses on the edge ecosystem, with the core report focusing on connecting and securing the entire edge computing ecosystem. This includes transport infrastructure, endpoints, operating systems, application workloads, and production monitoring/management/mitigation/runtime."

Akamai debuts Brand Protector service to combat phishing, online forgery

Source: https://www.csoonline.com/article/3694352/akamai-debuts-brand-protector-service-to-combat-phishing-online-forgery.html

From the Article: "Akamai is rolling out a new service designed to provide automated detection, investigation and even takedown services for businesses looking to protect their online reputations from digital criminals and phishing campaigns."

Ukraine cyber police arrested a man for selling data of 300M people

Source: https://securityaffairs.com/145406/cyber-crime/ukraine-cyber-police-arrested-man.html

From the Article: "The Ukrainian cyber police have arrested a man (36) from the city of Netishyn for selling the personal data and sensitive information of over 300 million people from different countries."

NI Peace Process accelerated it's rise as global cyber security hub, UK cyber chief explained at CYBERUK last week

Source: https://www.cybernewsgroup.co.uk/ni-peace-process-accelerated-its-rise-as-global-cyber-security-hub-uk-cyber-chief-explained-at-cyberuk-last-week/

Link back to Table of Contents

The articles have been 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: "Govt. chiefs have praised the significant role of the Belfast (Good Friday) Agreement in securing Northern Ireland's status as a global cyber security hub, as it continues to play a critical role in securing UK-wide online resilience 25 years after the pivotal accord was signed."

Weekly Cyber Threat Report, April 24 – 28, 2023

Source: https://cyberintelmag.com/threat-intelligence/weekly-cyber-threat-report-april-24-28-2023/

From the Article: "This week's good news includes CISA and Cyber Command working together to stop harmful cyberattacks, Google Authenticator App getting a TOTP Code Cloud Backup feature, critical updates from VMware being released for Workstation and Fusion software, PrestaShop resolving issues where any backend user may destroy databases, Ukrainian man being detained for selling the Russians information on 300 million individuals, and much more."

173K Developer Accounts Blocked by Google to Stop Malware And Fraud Rings

Source: https://cyberintelmag.com/malware-viruses/173k-developer-accounts-blocked-by-google-to-stop-malware-and-fraud-rings/

From the Article: "In order to prevent malware operations and fraud rings from infecting Android users' devices with fraudulent apps, Google claims that it banned 173,000 developer accounts in 2022."

Hackers From China Seen Using Linux PingPull Version in Targeted Cyberattacks

Source: https://cyberintelmag.com/attacks-data-breaches/hackers-from-china-seen-using-linux-pingpull-version-in-targeted-cyberattacks/

From the Article: "A new undocumented tool with the codename Sword2033 and a Linux backdoor variation known as PingPull are being used by the Chinese nation-state group known as Alloy Taurus."

PowerLess Backdoor Used by Iranian Hackers to Launch Sophisticated Attacks on Israel

Source: https://cyberintelmag.com/attacks-data-breaches/powerless-backdoor-used-by-iranian-hackers-to-launch-sophisticated-attacks-on-israel/

From the Article: "A revised version of a backdoor dubbed PowerLess is intended to be installed, and a new round of phishing attacks targeting Israel has been attributed to an Iranian nation-state threat actor. The hacker group known as APT35, Charming Kitten, Cobalt Illusion, ITG18, Mint Sandstorm (previously Phosphorus), TA453, and Yellow Garuda are among the groups that Check Point, a cybersecurity company, is keeping an eye on."

NSA sees 'significant' Russian intel gathering on European, U.S. supply chain entities

Source: https://cyberscoop.com/nsa-russian-ukraine-supply-chain-ransomware/

From the Article: "Russian hackers are focused on using ransomware to attack supply chains both within Ukraine and in European countries being used to provide weapons and humanitarian aid in support of the Ukrainian war effort, a top National Security Agency official said Wednesday."

Pro-Russian hacktivism isn't real, top Ukrainian cyber official says

Source: https://cyberscoop.com/pro-russia-hacktivism-ukraine/

From the Article: " In the wake of Russia's invasion of Ukraine, a flurry of pro-Russian "hacktivist" groups have claimed to carry out attacks on Russian enemies in a fit of patriotism."

US cybersecurity officials step up push for companies to adopt secure by design practices

Source: https://cyberscoop.com/secure-by-design-cyber-informed-engineering/

From the Article: "Top U.S. cybersecurity officials have been meeting with industry representatives and tech executives to press the need for companies to adopt secure by design principles that are a core part of the Biden administration's national cybersecurity strategy."

10 new and dangerous malware threats to watch out for (2023 edition)

Source: https://www.cybertalk.org/2023/04/25/10-new-and-dangerous-malware-threats-to-watch-out-for-2023-edition/

From the Article: "Discover 10 of the most dangerous malware threats and learn how to identify, prevent and defend against attacks."

Ransomware: Current state or already too late?

Source: https://www.cybertalk.org/2023/04/28/ransomware-current-state-or-already-too-late/

From the Article: "In this interview, Patrik Honegger, a Customer Advocacy Manager for Check Point, deep dives into the state of ransomware and recent trends. Discover practical steps for upgrading your ransomware prevention and defense programs to protect against serious and ever-evolving threats. Access expert knowledge and enhance your organization’s security measures."

Climate change, cyber security and saving the planet

Source: https://www.cybertalk.org/2023/04/19/climate-change-cyber-security-and-saving-the-planet/

From the Article: "In this article, we’ll explore key points pertaining to climate change and cyber security overlap and discuss steps that business leaders can take to mitigate risks and to build a more secure, sustainable and resilient future — all while addressing environmental, sustainability and governance (ESG) goals."

The US Cyber Command is Deploying Experts Abroad to Assist Collaborators in Detecting Hackers

Source: https://www.cysecurity.news/2023/04/the-us-cyber-command-is-deploying.html

From the Article: "The US government's Cyber National Command Force (CNCF) is deploying professionals abroad in "hunt forward" operations to assist partner countries in tackling cybercrime and has undertaken 47 operations in 20 countries in the last three years."

Link back to Table of Contents

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

Automated Bots Pose Growing Threat To Businesses

Source: https://www.cysecurity.news/2023/04/automated-bots-pose-growing-threat-to.html

From the Article: "The capability to detect, manage, and mitigate bot-based requests has become of utmost importance as cyber attackers become more automated. Edgio, a company created by the merging of Limelight Networks, Yahoo Edgecast, and Layer0, has unveiled its own bot management service in response to this expanding threat."

OFAC Takes Action Against Accused Providing Material Support To North Korean Hackers

Source: https://www.cysecurity.news/2023/04/ofac-takes-action-against-accused.html

From the Article: "The U.S. Treasury Department has recently identified three over-the-counter (OTC) cryptocurrency traders in China and Hong Kong, as well as a China-based banker, who is believed to have assisted North Korea's Lazarus Group in converting stolen crypto into fiat currency."

Decoy Dog Malware Toolkit: A New Cybersecurity Threat

Source: https://www.cysecurity.news/2023/04/decoy-dog-malware-toolkit-new.html

From the Article: "The U.S. Treasury Department has recently identified three over-the-counter (OTC) cryptocurrency traders in China and Hong Kong, as well as a China-based banker, who is believed to have assisted North Korea's Lazarus Group in converting stolen crypto into fiat currency."

Be Wary Because Cybercriminals Are Getting More Ingenious

Source: https://www.cysecurity.news/2023/04/be-wary-because-cybercriminals-are.html

From the Article: "In the media, misinformation is regularly discussed, primarily in relation to politics and is often used interchangeably with fake news. Even though these are major problems, a greater and more direct threat is frequently disregarded: how cybercriminals utilise false information to steal from businesses and people. "

Link back to Table of Contents

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

ChatGPT: A Game-Changer or a Cybersecurity Threat

Source: https://www.cysecurity.news/2023/04/chatgpt-game-changer-or-cybersecurity.html

From the Article: "The rise of artificial intelligence and machine learning technologies has brought significant advancements in various fields. One such development is the creation of conversational AI systems like ChatGPT, which has the potential to revolutionize the way people communicate with computers."

JupiterOne Weighs In On the Need For Unified Cyber Insights

Source: https://www.darkreading.com/cloud/jupiterone-weighs-in-on-the-need-for-unified-cyber-insights

From the Article: "JupiterOne founder Erkang Zheng joins Dark Reading's Terry Sweeney at Dark Reading News Desk during RSA Conference to discuss securing assets and attack surface management."

Your Attack Surface May Be Growing, But You Can Still Contain Your Risk

Source: https://www.darkreading.com/endpoint/your-attack-surface-may-be-growing-but-you-can-still-contain-your-risk

From the Article: "Lookout CEO Jim Dolce joins Dark Reading's Terry Sweeney at Dark Reading News Desk during RSA Conference to discuss remote work and the expanding attack surface."

Invicti Zooms In On Vulnerabilities That Plague Developers, Security Pros

Source: https://www.darkreading.com/application-security/invicti-zooms-in-on-vulnerabilities-that-plague-developers-security-pros

From the Article: "Invicti's Patrick Vandenberg joins Dark Reading's Terry Sweeney at Dark Reading News Desk during RSA Conference to discuss the latest global threat report."

Link back to Table of Contents

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

Firmware Looms as the Next Frontier for Cybersecurity

Source: https://www.darkreading.com/endpoint/firmware-looms-next-frontier-cybersecurity

From the Article: "Software bugs are ubiquitous, and we're familiar with hardware threats. But what about the gap in the middle? Two researchers at Black Hat Asia will attempt to focus our attention there."

CISO Survival Guide for Cyberattacks

Source: https://www.darkreading.com/vulnerabilities-threats/ciso-survival-guide-for-cyberattacks

From the Article: "CISOs who have survived major cyber incidents recommend letting company ethos guide incident response."

Tessian Fully Integrates With M365 To Provide Threat Protection and Insider Risk Protection

Source: https://www.darkreading.com/threat-intelligence/tessian-fully-integrates-with-m365-to-provide-threat-protection-and-insider-risk-protection

From the Article: " Tessian, a leading Integrated Cloud Email Security company, today announced the release of a new M365 Add-in, simplifying the deployment of the Tessian Cloud Email Security Platform."

'Anonymous Sudan' Claims Responsibility for DDoS Attacks Against Israel

Source: https://www.darkreading.com/attacks-breaches/anonymous-sudan-claims-responsibility-ddos-attacks-israel

From the Article: "The group has unleashed numerous attacks against the country during the week of Israel's Independence 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.

China's 'Evasive Panda' Hijacks Software Updates to Deliver Custom Backdoor

Source: https://www.darkreading.com/attacks-breaches/china-evasive-panda-hijacks-software-updates-custom-backdoor

From the Article: "Researchers observed downloads of installers for the APT's flagship backdoor, MgBot, when users at a Chinese NGO were updating legitimate applications."

SANS Reveals Top 5 Most Dangerous Cyberattacks for 2023

Source: https://www.darkreading.com/attacks-breaches/sans-lists-top-5-most-dangerous-cyberattacks-in-2023

From the Article: "SEO-aided attacks, developer targeting, and malicious use of AI top the list for 2023."

The White House National Cybersecurity Strategy Has a Fatal Flaw

Source: https://www.darkreading.com/vulnerabilities-threats/the-white-house-national-cybersecurity-strategy-has-a-fatal-flaw

From the Article: "The government needs to shift focus and reconsider how it thinks about securing our nation's digital and physical assets."

High-Severity SLP Flaw Can Amplify DDoS Attacks up to 2,200 Times

Source: https://www.darkreading.com/vulnerabilities-threats/high-severity-slp-flaw-can-amplify-ddos-attacks-up-to-2-200-times

From the Article: "More than 2,000 global organizations — including Fortune 1,000 companies — are at risk to reflective DDoS attacks that exploit a vulnerability discovered in the legacy Internet protocol."

Effects of the Hive Ransomware Group Takedown

Source: https://www.darkreading.com/vulnerabilities-threats/effects-of-the-hive-ransomware-group-takedown

Link back to Table of Contents

The articles have been 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: "Despite some success in limiting damage from Hive, there's no time to relax security vigilance."

Malware-Free Cyberattacks Are on the Rise; Here's How to Detect Them

Source: https://www.darkreading.com/endpoint/malware-free-cyberattacks-rise-how-to-detect

From the Article: "Last year, 71% of enterprise breaches were pulled off quietly, with legitimate tools, research shows."

Australians report record $3.1bn losses to scams, with real amount even higher, ACCC says

Source: https://www.theguardian.com/australia-news/2023/apr/17/australians-report-record-31bn-losses-to-scams-with-real-amount-even-higher-accc-says

From the Article: "Australians lost a record amount of more than $3.1bn to scams in 2022, up from the $2bn lost in 2021, a new report from the Australian Competition and Consumer Commission has revealed."

Ransomware Roundup - UNIZA Ransomware

Source: https://www.fortinet.com/blog/threat-research/ransomware-roundup-uniza-coverage

From the Article: "FortiGuardLabs examines the UNIZA ransomware, yet another variant that encrypts files on victims' machines in an attempt to extort money. Learn more in this week’s Ransomware Roundup."

Fortinet Helps Develop the Cyber Workforce of the Future

Source: https://www.fortinet.com/blog/business-and-technology/fortinet-develops-future-cybersecurity-workforce

From the Article: "See how the Fortinet Training Institute partners with academic institutions to develop the future cybersecurity workforce with the skills they need to excel in the industry."

Google Adds New Cyber Security Tools & Features to ChromeOS

Source: https://gbhackers.com/chromeos-security-tools/

From the Article: "As per reports, cybercrime will reach $10.5 trillion by 2025, including all kinds of cybercrime activities like RaaS, Phishing, malware, and much more. It will be mandatory for organizations to protect themselves from these threats."

Cosmos Bank Cyber Attack – 11 Accused in Cyber Fraud Case

Source: https://gbhackers.com/cosmos-bank-cyber-attack/

From the Article: "The Cosmos cooperative bank in Pune, among the city’s oldest urban cooperative banks, has fallen prey to cyber fraudsters. Hackers gained access to the bank’s system and stole Rs 94 crore."

New Phishing Attacks Using ChatGPT to Develop Sophisticated Campaigns

Source: https://gbhackers.com/new-phishing-attacks/

From the Article: "Phishing has been one of the greatest threats to organizations, growing year after year. Phishing attacks have contributed to 90% of data breaches in the past few years, which makes cybercriminals adapt to them, making their attacks much more successful."

Celebrating SLSA v1.0: securing the software supply chain for everyone

Source: http://security.googleblog.com/2023/04/celebrating-slsa-v10-securing-software.html

From the Article: "Last week the Open Source Security Foundation (OpenSSF) announced the release of SLSA v1.0, a framework that helps secure the software supply chain. Ten years of using an internal version of SLSA at Google has shown that it’s crucial to warding off tampering and keeping software secure."

Link back to Table of Contents

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

"Ashamed" LockBit ransomware gang apologises to hacked school, offers free decryption tool

Source: https://www.bitdefender.com/blog/hotforsecurity/ashamed-lockbit-ransomware-gang-apologises-to-hacked-school-offers-free-decryption-tool/

From the Article: "Last month, a school district in Illinois was reported to be working closely with a cybersecurity insurance firm to determine the extent of damage it had sustained from a ransomware attack."

Pro-Russia hackers attack European air traffic control website, but don't panic! Flights continue as normal

Source: https://www.bitdefender.com/blog/hotforsecurity/pro-russia-hackers-attack-european-air-traffic-control-website-but-dont-panic-flights-continue-as-normal/

From the Article: "Eurocontrol, the European air traffic control agency, has revealed that it has been under cyber attack for the last week, and says that pro-Russian hackers have claimed responsibility for the disruption."

One Brooklyn Reports Breach, Faces Lawsuit Post-Cyberattack

Source: https://www.bankinfosecurity.com/one-brooklyn-reports-breach-faces-lawsuit-post-cyberattack-a-21907

From the Article: "One Brooklyn Health is facing a proposed class action lawsuit in the wake of a data breach affecting more than 235,000 individuals, which the organization reported to regulators following a cyberattack late last year that disrupted its IT systems and patient services for several weeks."

New England Health Plan Still Recovering From Attack

Source: https://www.bankinfosecurity.com/point32health-attack-a-21895

From the Article: "Point32Health, which provides health plans to millions of New Englanders and is Massachusetts' second-largest health insurer, is still struggling to recover 10 days after it identified a ransomware attack that forced the company to take many of its IT systems and functions offline."

Hackers Exploit TP-Link N-Day Flaw to Build Mirai Botnet

Source: https://www.bankinfosecurity.com/hackers-exploit-tp-link-n-day-flaw-to-build-mirai-botnet-a-21866

From the Article: "Hackers are attempting to infect a consumer-grade Wi-Fi router model with Mirai botnet malware following the discovery of zero-days in the device in a December hacking competition."

Obscure Network Protocol Has Flaw That Could Unleash DDoS

Source: https://www.bankinfosecurity.com/obscure-network-protocol-has-flaw-that-could-unleash-ddos-a-21863

From the Article: "An obscure routing protocol codified during the 1990s has come roaring back to attention after researchers found a flaw that would allow attackers to initiate massive distributed denial-of-service attacks. Researchers from Bitsight and Curesec say they found a bug in Service Location Protocol."

Medtronic Reports InPen Mobile Diabetic App Tracking Breach

Source: https://www.bankinfosecurity.com/medtronic-breach-a-21849

From the Article: "Diabetic patients who used a Medtronic smartphone app for managing insulin levels are being told that Google may have collected certain personal information through the sign-in infrastructure."

SECURITY ALERT: Heimdal® Identifies Active Phishing Campaign Singleing Out Romanian Telecom Users

Source: https://heimdalsecurity.com/blog/active-phishing-campaign/

From the Article: "On the 28th of April, acting on a tip received from an anonymous source, Heimdal®'s SOC team has come across an active phishing campaign that appears to specifically target Romanian telecom customers. "

Managed Threat Hunting: The Next Step from Traditional Cybersecurity

Source: https://heimdalsecurity.com/blog/managed-threat-hunting/

From the Article: "As the world becomes increasingly digital, cybersecurity threats continue to evolve and become more sophisticated. Traditional cybersecurity measures are no longer enough to protect organizations from malicious attacks."

TP-Link High-Severity Flaw Added to Mirai Botnet Arsenal

Source: https://heimdalsecurity.com/blog/tp-link-high-severity-flaw-added-to-mirai-botnet-arsenal/

From the Article: "A TP-Link Archer A21 (AX1800) consumer-grade WiFi router vulnerability has been used by Mirai botnet to launch DDoS attacks against IoT devices. The flaw in the TP-Link Archer AX21 firmware was discovered back in December 2022, and the company released a patch in March."

New LOBSHOT Malware Deployed Via Google Ads

Source: https://heimdalsecurity.com/blog/new-lobshot-malware-deployed-via-google-ads/

From the Article: "Google advertisements have been exploited to distribute various types of malware over the past few months. To trick unsuspecting users into downloading malware onto their systems, threat actors often used the platform to promote fake websites on legit software and application updates."

7,413 People Were Impacted by Alaska Railroad Data Breach

Source: https://heimdalsecurity.com/blog/alaska-railroad-data-breach/

From the Article: "Alaska Railroad Corporation reported a data breach incident that occurred in December 2022 and they discovered it on March 18th, 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.

IMA Financial Group Targeted in Cyberattack. Confidential Consumer Data Spilled

Source: https://heimdalsecurity.com/blog/ima-financial-data-breach/

From the Article: "IMA Financial Group (IMA) announced on April 19th it had experienced a data breach resulting in confidential consumer data leakage. The insurance and wealth management solutions company filed a notice of the data security incident with the Attorney General of Texas. "

New Type of Side-Channel Attack Impacts Intel CPUs and Allows Data Leakage

Source: https://heimdalsecurity.com/blog/new-type-of-side-channel-attack-impacts-intel-cpus-and-allows-data-leakage/

From the Article: "Researchers discovered a new kind of side-channel attack that affects several versions of Intel CPUs and enables data exfiltration. Attackers could leak the data through the EFLAGS register."

Week in review: PaperCut vulnerabilities, VMware fixes critical flaws, RSA Conference 2023

Source: https://www.helpnetsecurity.com/2023/04/30/week-in-review-papercut-vulnerabilities-vmware-fixes-critical-flaws-rsa-conference-2023/

From the Article: "Here’s an overview of some of last week’s most interesting news, articles, interviews and videos: RSA Conference 2023 RSA Conference 2023 took place at the Moscone Center in San Francisco."

UK Cyber Security Council launches certification mapping tool

Source: https://www.helpnetsecurity.com/2023/04/30/uk-cyber-security-council-certification-mapping-tool/

From the Article: "The UK Cyber Security Councilv has launched the first phase of its certification mapping tool. It has been created to map all available cyber security certifications onto the 16 specialisms identified by the Council, with the first phase now available. "

Link back to Table of Contents

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

Codenotary unveils SBOMcenter to ensure software supply chain security

Source: https://www.helpnetsecurity.com/2023/04/29/codenotary-sbomcenter/

From the Article: "Codenotary has unveiled SBOMcenter, providing a central, secure place for software producers and consumers to freely generate, store and share Software Bills of Materials (SBOMs)."

Phishing-resistant MFA shapes the future of authentication forms

Source: https://www.helpnetsecurity.com/2023/04/28/phishing-resistant-mfa-authentication-forms/

From the Article: "Over the last two years, respondents reported a continued reliance on the least secure forms of authentication, including traditional usernames and passwords and one-time passwords (OTPs), according to Yubico."

Cybersecurity leaders introduced open-source information sharing to help OT community

Source: https://www.helpnetsecurity.com/2023/04/26/ethos-open-source-platform/

From the Article: "A group of OT cybersecurity leaders and critical infrastructure defenders introduced their plans for ETHOS (Emerging THreat Open Sharing), an open-source, vendor-agnostic technology platform for sharing anonymous early warning threat information across industries with peers and governments."

Graylog 5.1 optimizes threat detection and response

Source: https://www.helpnetsecurity.com/2023/04/26/graylog-5-1-platform/

From the Article: "Graylog announced at the RSA Conference 2023 Graylog 5.1 with new incident investigation and enhancements to its cybersecurity solution. Currently available in Beta, version 5.1 of Graylog Security and the Graylog Platform will be GA in May 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.

Eclypsium launches Supply Chain Security Platform with SBOM capability

Source: https://www.helpnetsecurity.com/2023/04/26/eclypsium-supply-chain-security-platform/

From the Article: "Eclypsium released Supply Chain Security Platform, enabling an organization's IT security and operations teams to continuously identify and monitor the bill of materials, integrity and vulnerability of components and system code in each device, providing insight into the overall supply chain risk to the organization."

ExtraHop simplifies approach to intrusion detection for security teams with new solutions

Source: https://www.helpnetsecurity.com/2023/04/26/extrahop-ids/

From the Article: "ExtraHop launched ExtraHop IDS, which integrates with the ExtraHop Reveal(x) platform to offer a new, simplified approach to intrusion detection for deeper coverage and full-spectrum investigation. As part of its release, ExtraHop also announced several product enhancements, including Automated Retrospective Detection and a native integration with Palo Alto Cortex XSOAR."

Akamai Prolexic Network Cloud Firewall defends organizations against DDoS attacks

Source: https://www.helpnetsecurity.com/2023/04/26/akamai-prolexic-network-cloud-firewall/

From the Article: "Akamai launched Prolexic Network Cloud Firewall, allowing customers to define and manage their own access control lists (ACLs) while enabling greater flexibility to secure their own network edge."

Deep Instinct partners with eSentire to protect customers from unknown and zero-day attacks

Source: https://www.helpnetsecurity.com/2023/04/26/deep-instinct-esentire/

From the Article: "Deep Instinct announced a new partnership with eSentire to protect eSentire customers from unknown and zero-day attacks. As ransomware and data exfiltration become more prevalent and damaging to businesses, the need for proactive cybersecurity has never been greater."

Most SaaS adopters exposed to browser-borne attacks

Source: https://www.helpnetsecurity.com/2023/04/25/saas-adopters-exposed-browser-borne-attacks/

From the Article: "Even though the adoption of SaaS apps started more than ten years ago, CISOs are still finding it challenging to tackle the accumulated security debt. Significant deficiencies The prevalence of phishing and account takeover attacks has raised significant concerns, as most organizations have experienced them within the last year."

VMware announces new security capabilities to help protect hybrid workforce

Source: https://www.helpnetsecurity.com/2023/04/25/workspace-one-vmware/

From the Article: "VMware has unveiled new capabilities that deliver lateral security across multi-cloud environments so customers can better see and stop more threats and innovations to its Workspace ONE platform that will better enable organizations to secure their hybrid workforce."

Despite Soaring Prices, Cybersecurity Insurance Keeps Growing Briskly

Source: https://www.tripwire.com/state-of-security/despite-soaring-prices-cybersecurity-insurance-keeps-growing-briskly

From the Article: "Most cybersecurity professionals know that cyber breaches increase each year. So it’s no surprise that the cybersecurity insurance business also keeps growing briskly. According to data from Markets and Markets and Polaris Market Research, the cyber insurance market swelled to $11.9 billion worldwide in 2022, up from $10.1 billion the previous year, and is projected to grow to more than $29 billion by 2027."

Evaluating ICS cyber threat landscape focusing on insider threats in OT environments

Link back to Table of Contents

Source: https://industrialcyber.co/features/evaluating-ics-cyber-threat-landscape-focusing-on-insider-threats-in-ot-environments/

From the Article: "Operational technology (OT) environments face numerous cybersecurity risks and threats, such as supply chain security threats, nation-state hackers, malware, ransomware, and ransomware-as-a-service (RaaS) attacks, and data breaches, which can potentially disrupt services and halt production lines. "

BitDefender details Charming Kitten's BellaCiao malware targeting multiple victims in US, Europe, Middle East, India

Source: https://industrialcyber.co/ransomware/bitdefender-details-charming-kittens-bellaciao-malware-targeting-multiple-victims-in-us-europe-middle-east-india/

From the Article: "Researchers from Bitdefender Labs identified the modernization of Charming Kitten's tactics, techniques, and procedures (TTPs), including a new, previously unseen malware called BellaCiao. "

MITRE Caldera for OT tool streamlines cybersecurity assessments, helps defenders better respond to adversary behavior

Source: https://industrialcyber.co/ics-security-framework/mitre-caldera-for-ot-tool-streamlines-cybersecurity-assessments-helps-defenders-better-respond-to-adversary-behavior/

From the Article: "Not-for-profit organization MITRE released at the ongoing RSA 2023 conference its MITRE Caldera for OT tool that allows security teams to run automated adversary emulation exercises targeted against OT (operational technology) environments."

Nozomi joins Accenture Security, IBM Security, Mandiant on Elite Cyber Defenders Program

Source: https://industrialcyber.co/critical-infrastructure/nozomi-joins-accenture-security-ibm-security-mandiant-on-elite-cyber-defenders-program/

From the Article: "Industrial cybersecurity vendor Nozomi Networks announced Tuesday its new Elite Cyber Defenders Program, with Accenture Security, IBM Security, and Mandiant (now part of Google Cloud) as initial participants."

Link back to Table of Contents

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

A Comprehensive Look At Email-Based Threats In 2023

Source: https://informationsecuritybuzz.com/a-comprehensive-look-at-email-based-threats-in-2023/

From the Article: "It follows that vectors with greater internet exposure will also attract more attention from threat actors. Because of this, malicious actors frequently exploit public email servers, and a wide variety of cyber dangers can spread through them."

50 Crypto Wallets Targeted by Atomic MacOS Malware

Source: https://informationsecuritybuzz.com/50-crypto-wallets-targeted-by-atomic-macos-malware/

From the Article: "Security professionals have issued alerts regarding a new type of malware that targets MacOS devices in an effort to steal sensitive data, including credit card details, credit card expiration dates, and information from over 50 Bitcoin browser extensions. "

Good, Better And Best Security

Source: https://informationsecuritybuzz.com/good-better-and-best-security/

From the Article: "What does a “good” cyber-security programme look like? How can we, in our role as Chief Information Security Officer (CISO), work to improve the effectiveness of the policies and practices implemented in our organisations? "

RCE Attacks Against Thousands Of Apache Superset Servers

Source: https://informationsecuritybuzz.com/rce-attacks-against-thousands-of-apache-superset-servers/

From the Article: "At its default settings, Apache Superset is vulnerable to authentication bypass and remote code execution, allowing attackers to read and alter data, gather passwords, and issue commands."

Link back to Table of Contents

Large 2,200x DDoS Amplification Assault Due To New SLP Flaw

Source: https://informationsecuritybuzz.com/large-2200x-ddos-amplification-assault-new-slp-flaw/

From the Article: "Threat actors can conduct enormous denial-of-service attacks with 2,200X amplification thanks to a new reflected Denial-of-Service (DoS) increasing its vulnerability in the Service Location Protocol (SLP). Researchers at BitSight and Curesec identified this weakness as CVE-2023-29552."

Vietnamese Hackers Linked to 'Malverposting' Campaign

Source: https://www.infosecurity-magazine.com/news/vietnamese-hackers-malverposting/

From the Article: "Security experts at Guardio Labs discussed the findings in a new blog post."

Evasive Panda's Backdoor MgBot Delivered Via Chinese Software Updates

Source: https://www.infosecurity-magazine.com/news/evasive-panda-mgbot-delivered-via/

From the Article: "Most of the plugins are designed to steal information from highly popular Chinese applications."

New SLP Vulnerability Could Enable Massive DDoS Attacks

Source: https://www.infosecurity-magazine.com/news/new-slp-vulnerability-massive-ddos/

From the Article: "Bug has potential to facilitate 2200x amplification attacks."

Google Joins AI Cybersecurity Party with Cloud Security Workbench

Source: https://www.itgovernanceusa.com/blog/google-joins-ai-cybersecurity-party-with-cloud-security-workbench

From the Article: "The stratospheric rise of artificial intelligence over the past six months has been a sight to behold. Following the release of ChatGPT in October 2022, a platform that produces content at a whim, ranging from essay answers, blog posts, and sort-of-functional code, practically every major player in the tech industry has thrown their hat into the ring."

Email Threat Report 2023: Key Takeaways

Source: https://www.itsecurityguru.org/2023/04/27/email-threat-report-2023-key-takeaways/

From the Article: "Every day, countless people across all industries send and receive emails as a significant part of their jobs. Email is often the most convenient and simplest way to get keep in contact with key stakeholders such as co-workers, senior management, and clients, and many don't give it a second thought. However, the state of email security is rife with risks."

Latest QBot Attacks Use a Mixture of PDF Attachments and Windows Scripting Host Files to Infect Victims

Source: https://blog.knowbe4.com/qbot-attacks-pdfs-windows-scripting-host-files

From the Article: "QBot malware seems to be outliving its competitors through innovative new ways to socially engineer victims into helping install it."

Despite a Majority of Organizations Believing They're Prepared for Cyber Attacks, Half Were Still Victims

Source: https://blog.knowbe4.com/cyber-attack-preparedness-overconfidence

From the Article: "A new survey points to an overconfidence around organization's preparedness, despite admitting to falling victim to ransomware attacks – in some cases multiple times."

Organizations Have No Idea of a Data Breach's Root Cause in 42% of Reported Cases

Link back to Table of Contents

Source: https://blog.knowbe4.com/data-breach-root-causes-unknown

From the Article: "New data shows how poorly organizations are at identifying – let alone removing – an attacker's foothold, putting themselves at continued risk of further attacks and data breaches."

Decoy Dog Malware Tool Kit Spotted Via Malicious DNS Queries

Source: https://latesthackingnews.com/2023/04/26/decoy-dog-malware-tool-kit-spotted-via-malicious-dns-queries/

From the Article: "A new malware tool kit, “Decoy Dog,” has been actively targeting enterprise networks for a year. The researchers identified Decoy Dog after analyzing billions of DNS queries."

AuKill Malware Actively Used To Disable EDR In Ongoing Attacks

Source: https://latesthackingnews.com/2023/04/28/aukill-malware-actively-used-to-disable-edr-in-ongoing-attacks/

From the Article: "Researchers have discovered a new malware that remained under the radar for quite some time."

Evil Extractor Infostealer Targets Windows In Recent Phishing Campaign

Source: https://latesthackingnews.com/2023/04/24/evil-extractor-infostealer-targets-windows-in-recent-phishing-campaign/

From the Article: "Researchers observed malicious use of a self-claimed educational tool, “Evil Extractor,” for stealing data. "

onsemi and ZEEKR sign long-term supply agreement for silicon carbide power devices

Source: https://www.semiconductor-today.com/news_items/2023/apr/onsemi-260423.shtml

From the Article: "Power semiconductor IC supplier onsemi of Phoenix, AZ, USA has announced a long-term supply agreement (LTSA) to provide its EliteSiC silicon carbide (SiC) power devices to increase the powertrain efficiency of smart electric vehicles (EVs) made by ZEEKR (the global premium electric mobility brand of China-based Geely Holding Group)."

iOS Lockdown Mode effective against NSO zero-click exploit

Source: https://www.malwarebytes.com/blog/news/2023/04/ios-lockdown-mode-effective-against-nso-zero-click-exploit

From the Article: "This is a huge deal since it shows how useful Lockdown Mode can be, even against exploits developed by one of the world's most notorious commercial spyware producers."

Fileless attacks: How attackers evade traditional AV and how to stop them

Source: https://www.malwarebytes.com/blog/business/2023/04/fileless-attacks-how-attackers-evade-traditional-av-and-how-to-stop-them

From the Article: "When you hear about malware, there's a good chance you think of sketchy executables or files with extensions like .DOCX or .PDF that, once opened, execute malicious code. These are examples of file-based attacks—and while they can be bad, they're nothing compared to their fileless cousins."

Healthy security habits to fight credential breaches: Cyberattack Series

Source: https://www.microsoft.com/en-us/security/blog/2023/04/26/healthy-security-habits-to-fight-credential-breaches-cyberattack-series/

From the Article: "Fifty percent of Microsoft cybersecurity recovery engagements relate to ransomware,1 and 61 percent of all breaches involve credentials.2 In this second report in our ongoing Cyberattack Series, we look at the steps taken to discover, understand, and respond to a push-bombing request that targeted a legitimate user, allowing an attacker to authenticate and register their own mobile device."

Why you should practice rollbacks to prevent data loss in a ransomware attack

Source: https://www.microsoft.com/en-us/security/blog/2023/04/27/why-you-should-practice-rollbacks-to-prevent-data-loss-in-a-ransomware-attack/

From the Article: "In the latest post of our Community Voices blog series, Microsoft Security Senior Product Marketing Manager Brooke Lynn Weenig talks with Tanya Janca, Founder and Chief Executive Officer (CEO) of We Hack Purple, who is known as SheHacksPurple and is the best-selling author of Alice and Bob Learn Application Security."

100% Increase in DDoS Attacks Against india

Source: https://www.netscout.com/blog/asert/100-increase-ddos-attacks-against-india

From the Article: "Summary NETSCOUT and ASERT have observed massive increases in DDoS attacks against Indian targets. This near doubling of DDoS attacks since the beginning of 2023 has been fueled by a rallying call from hacker groups Anonymous Sudan and Killnet."

Sifting Through The Top Cyber Myths In The Military Service Branches

Source: https://www.scmagazine.com/analysis/careers/top-cyber-myths-military-service-branches

From the Article: "When Congress passed legislation in 2020 mandating the creation of principal cyber advisor (PCA) roles throughout each of the service branches, they did so with an eye towards centralizing and coordinating planning and funding for cyber operations across the military."

Western Digital hit by hackers

Source: https://www.pandasecurity.com/en/mediacenter/security/western-digital/

From the Article: "Last month Western Digital (WD) was hit by a hacker attack. TechCrunch first reported the news on Thursday last week after the cybercriminals contacted the popular blog. WD is known as a Silicon Valley-based American computer drive manufacturer and data storage company."

Link back to Table of Contents

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

Qualys Virtual Cyber Risk Summit: That’s a Wrap!

Source: https://blog.qualys.com/qualys-insights/2023/04/27/qualys-virtual-cyber-risk-summit-thats-a-wrap

From the Article: "Over the last few years, the volume of software developed and the surge in vulnerabilities has been staggering. Combine this with a shortage of cybersecurity professionals, and organizations are left with the daunting challenge of keeping up with the sheer volume of information coming at them. "

Make Sure You Have These Analysis Tools That Are in Radware’s DDoS Management Solution

Source: https://blog.radware.com/security/ddos/2023/04/analysis-tools-needed-in-a-ddos-management-solution/

From the Article: "One of the most commonly overlooked topics when selecting a DDoS protection solution relates to analytics and reporting tools. Many customers choose a DDoS solution based solely on either how effective they believe it will be or how well they’ve been told it protects against various attacks."

Stronger cybersecurity, reducing cyber incidents, greater EU 'strategic autonomy'? Three ...

Source: https://www.databreaches.net/stronger-cybersecurity-reducing-cyber-incidents-greater-eu-strategic-autonomy-three-interesting-features-of-the-proposed-eu-cyber-solidarity-act/

From the Article: "The CSA adds another layer to the increasingly crowded landscape of EU cybersecurity laws. The proposed law would interact with the revised Network and Information Security Directive (“NIS2”) and certifications issued under the Cybersecurity Act."

London casino reopening date nearing, two weeks after ransomware attack

Source: https://lfpress.com/news/local-news/london-casino-reopening-date-nearing-two-weeks-after-ransomware-attack

From the Article: "The casino company that runs operations in London and across

Ontario has slowly started reopening locations after a two-week shutdown following a ransomware attack by hackers."

The groups of cybercriminals that sow chaos in Spain and the world in the spotlight - Gearrice

Source: https://www.gearrice.com/update/the-groups-of-cybercriminals-that-sow-chaos-in-spain-and-the-world-in-the-spotlight/

From the Article: "Cyber attacks have never been more complex, more profitable, and perhaps even more baffling. “The ongoing geopolitical storm brings with it not only the classic cyber threats to businesses, but also unpredictable risks and ‘black swans'”add Kaspersky sources."

Ransomware and vulnerability of the pharma industry - Risk - Asia Insurance Review

Source:
https://www.asiainsurancereview.com/Magazine/ReadMagazineArticle?aid=46648

From the Article: "Ransomware attacks against Indian pharma companies are on the rise, however, it appears that the industry does not view this threat with the seriousness it deserves."

Who Knows .dypgomzz ransomware - Bleeping Computer

Source: https://www.bleepingcomputer.com/forums/t/784965/who-knows-dypgomzz-ransomware/

From the Article: "Unfortunately, there is no known method that I am aware of to decrypt files encrypted by Magniber 2022 without paying the ransom (not advisable) and obtaining the private encryption keys from the criminals who created the ransomware unless they are leaked or seized & released by authorities."

Cyberattacks fall sharply in Vietnam - Vietnamnet

Source: https://vietnamnet.vn/en/cyberattacks-fall-sharply-in-vietnam-2138074.html

Link back to Table of Contents

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

From the Article: "The cybercrime situation in Southeast Asia in 2022 was complicated. The latest data from Kaspersky showed that the security company successfully prevented 12.38 million cyberattacks against the websites of Southeast Asian businesses last year."

Cybersecurity: 7 Online Safety Terms Everyone Should Know - World Nation News

Source: https://worldnationnews.com/cybersecurity-7-online-safety-terms-everyone-should-know/

From the Article: "In the context of an increasingly digitized society, the cyber security It has become a key issue. To help users better understand the risks and protect themselves, we have created a list of seven key cybersecurity terms that are important to know. From phishing to malware, learn how these concepts can affect your digital life and how to protect yourself."

5 Reasons to Look for Cyber Security Solutions in the Pharma Industry - Analytics Insight

Source: https://www.analyticsinsight.net/5-reasons-to-look-for-cyber-security-solutions-in-the-pharma-industry/

From the Article: "One of the most significant global industries is the pharmaceutical sector, and as digital technology is used more frequently, the need for cybersecurity solutions is growing. "

Select Board receives cybersecurity presentation | News - Homenewshere.com

Source: http://homenewshere.com/wilmington_town_crier/news/article_127a332a-e479-11ed-aef0-d3cd94f137d0.html

From the Article: "Wil-mington’s IT Director John O’Neil provided a presentation to the Sel-ect Board at their meeting on Monday night. He presented two recent initiatives coming out of the IT department."

From Phishing To Malware, 7 Important Cyber Security Terms Everyone Should Know

Source: https://nationworldnews.com/from-phishing-to-malware-7-important-cyber-security-terms-everyone-should-know/

From the Article: "Before addressing the topic, you can review it Depor Technology Portal For more cyber security tips. In a recent report, we shared some things to consider when creating passwords and how often you should change them."

Hackers target vulnerable Veeam backup servers exposed online - Bleeping Computer

Source: https://www.bleepingcomputer.com/news/security/hackers-target-vulnerable-veeam-backup-servers-exposed-online/

From the Article: "Malicious activity and tools echoing FIN7 attacks have been observed in intrusions since March 28, less than a week after an exploit became available for a high-severity vulnerability in Veeam Backup and Replication (VBR) software."

Russian ransomware attack software targets Apple Mac and MacBook - Vigour Times

Source: https://vigourtimes.com/russian-ransomware-attack-software-targets-apple-mac-and-macbook/

From the Article: "LockBit, a type of ransomware, is one of the first known instances of this malware targeting Mac computers. It is also one of the most widely-used ransomware known today, and its creators are offering cybercriminals this ransomware as a service, which allows various hacking groups to use it for a price. "

Rapture, a Ransomware Family With Similarities to Paradise - Trend Micro

Source: https://www.trendmicro.com/en_us/research/23/d/rapture-a-ransomware-family-with-similarities-to-paradise.html

From the Article: "In March and April 2023, we observed a type of ransomware targeting its victims via a minimalistic approach with tools that leave only a minimal footprint behind. Our findings revealed many of the preparations made by the perpetrators and how quickly they managed to carry out the ransomware attack."

Axios on Twitter: "Ransomware — a novelty just a few years ago — is now endemic, like

COVID ...

Source: https://twitter.com/axios/status/1652097834080927746

From the Article: "Ransomware attacks have exacted an escalating price on law enforcement, policymaking and financial resources."

Chinese tech firm launches cyber security solution software in Kenya

Source: https://www.bignewsnetwork.com/news/273794615/chinese-tech-firm-launches-cyber-security-solution-software-in-kenya

From the Article: "Chinese tech firm Huawei on Friday launched its latest cyber security service targeting the Kenyan private and public sectors, deepening the use of cloud storage solutions and artificial intelligence systems amid escalating cyber attacks."

Cyber Security Today, Week in Review for the week ending Friday, April 28, 2023

Source: https://www.itworldcanada.com/article/cyber-security-today-week-in-review-for-the-week-ending-friday-april-28-2023/537726

From the Article: "Welcome to Cyber Security Today. This is the week in Review edition for the week ending Friday, Arpil 28th, 2023. I'm Howard Solomon, cybersecurity reporter for ITWorldCanada.con and TechNewsday.com in the U.S."

United HealthCare data breach may have revealed personal information of customers

Source: https://news.yahoo.com/united-healthcare-data-breach-may-235746010.html

From the Article: "A breach, which happened between Feb 19 and Feb 25, may have disclosed personal information of healthcare plan members that included first and last names, addresses, date of birth and provider names."

Tonto Team Uses Anti-Malware File to Launch Attacks on South Korean Institutions

Source: https://thehackernews.com/2023/04/tonto-team-uses-anti-malware-file-to.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: "South Korean education, construction, diplomatic, and political institutions are at the receiving end of new attacks perpetrated by a China-aligned threat actor known as the Tonto Team."

Huawei releases first network-storage ransomware protection solution in Kenya - KBC

Source: https://kbc.co.ke/technology/article/38388/huawei-releases-first-network-storage-ransomware-protection-solution-in-kenya

From the Article: "Chinese tech giant Huawei on Friday launched the industry's first multilayer ransomware protection solution based on network-storage collaboration during an event to mark the Huawei ICT Day 2023 in Nairobi."

Breach roundup. Hackers steal more than hearts. - CyberWire

Source: https://thecyberwire.com/newsletters/privacy-briefing/5/82

From the Article: "Bank Info Security offers a roundup of recent cyberincident news, including the arrest in Ukraine of a man accused of selling the personal data of over 300 million individuals."

Cyber-attackers are 'logging in' instead of breaking in: Report - ITP.net

Source: https://www.itp.net/security/cyber-attackers-are-logging-in-instead-of-breaking-in-report

From the Article: "Ransomware was also the culprit in 75 percent of Sophos' IR investigations over the last three years."

Mandiant Report: Dwell Time Decreases While Ransomware, Extortion Flourish

Source: https://www.darkreading.com/vulnerabilities-threats/mandiant-report-dwell-time-decreases-while-ransomware-extortion-flourish

From the Article: "Mandiant's Charles Charmakal digs into the findings from the company's latest annual M-Trends report, noting that average dwell time has decreased to 16 days. He discusses whether most companies are detecting threats independently or are waiting to be alerted. Charmakal also describes the latest moves in online extortion and ransomware."

Ontario casino ransomware attack 'as bad as it gets,' expert says - iHeartRadio

Source: https://barrie.ctvnews.ca/ontario-casino-ransomware-attack-as-bad-as-it-gets-expert-says-1.6375498

From the Article: "Technology analyst Carmi Levy said the situation is the digital equivalent of recovering from a major fire or similar disaster."

NBC 10 I-Team: Investigation into North Kingstown ransomware attack in full swing | WJAR

Source: https://turnto10.com/i-team/north-kingstown-cyberattack-ransomware-municipal-computers-laptops-data-cloud-security-upgrades-rhode-island

From the Article: "North Kingstown is in recovery mode after being targeted by a ransomware attack last weekend."

CA Health Plan Reports Data Breach Tied to Fortra GoAnywhere Hack - Health IT Security

Source: https://healthitsecurity.com/news/ca-health-plan-reports-data-breach-tied-to-fortra-goanywhere-hack

From the Article: "California-based Santa Clara Health Plan (SCHP) reported a breach tied to a known vulnerability in Fortra's GoAnywhere managed file transfer (MFT) solution that impacted 276,993 individuals. As previously reported, threat actors have been leveraging the vulnerability to gain access to sensitive data."

Ransomware attacks are up significantly in the first months of 2023 - The Jerusalem Post

Source: https://www.jpost.com/business-and-innovation/tech-and-start-ups/article-741560

From the Article: "In March of this year, 410 people reported that they had been a victim of ransomware attacks, indicating a significant increase compared to the 208 reported victims of April 2022. Additionally, the numbers from March were 1.6 times higher than those reported in the peak month of 2022, the first annual Ransomware Threat Landscape Report published Monday by Black Kite Research has shown."

Cybersecurity Trends in 2023 - EisnerAmper

Source: https://www.eisneramper.com/cybersecurity-trends-0423/

From the Article: "Cybercrime attacks are becoming more sophisticated as new technological innovations are brought to market. Artificial intelligence is one of the most prominent technological innovations to impact cybercrime, and will continue to be a major concern for individuals, businesses and governments."

The Week in Ransomware - April 28th 2023 - Clop at it again

Source: https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-april-28th-2023-clop-at-it-again/

From the Article: "It has been a very quiet week for ransomware news, with only a few reports released and not much info about cyberattacks."

Report Shows Malware Attacks on the Rise in Higher Education | EdTech Magazine

Source: https://edtechmagazine.com/higher/article/2023/04/report-shows-malware-attacks-rise-higher-education

From the Article: "The education sector was among the top industries impacted by cybercrime in 2022, according to the 2023 SonicWall Cyber Threat Report. The report collected real-world data from SonicWall’s Capture Threat Network, which monitors and collects information from more than 1.1 million sensors across the company’s global devices."

Organizations Face Increased Scrutiny of Health Data Breaches - The HIPAA Journal

Source: https://www.hipaajournal.com/organizations-face-increased-scrutiny-of-health-data-breaches/

Link back to Table of Contents

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

From the Article: "Healthcare hacking incidents are increasing, there are new regulatory requirements and compliance initiatives due to Dobbs and Pixel use, and lawsuits against healthcare organizations over privacy violations are soaring."

Cyber insurance cannot replace robust cyber risk management - ITWeb

Source: https://www.itweb.co.za/content/xnklOvz1KkYq4Ymz

From the Article: "Cyber security company Fortinet says companies should invest in cyber insurance to claim back on financial loss from cyber attacks, but this is only a way to minimise damage and can make organisations more attractive to cyber criminals."

LockBit Leads as Rampant Ransomware Activity Continues - Security Boulevard

Source: https://securityboulevard.com/2023/04/lockbit-leads-as-rampant-ransomware-activity-continues/

From the Article: "Ransomware actors continue to focus their attacks on the manufacturing sector, and LockBit remains the most prolific threat group, according to the results of the GuidePoint Research and Intelligence Team’s (GRIT) Q1 2023 ransomware report."

The Good, the Bad and the Ugly in Cybersecurity - Week 17 - SentinelOne

Source: https://www.sentinelone.com/blog/the-good-the-bad-and-the-ugly-in-cybersecurity-week-17-4/

From the Article: "This was the week that was RSAC 2023, so good news abounded aplenty as vendors across the cybersecurity space made announcements and reveals about new features, services and products designed to help defenders keep their enterprises safe."

Report: Ransomware attacks see resurgence in 2023 - Security Magazine

Source: https://www.securitymagazine.com/articles/99271-report-ransomware-attacks-see-resurgence-in-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: "In its new report, Ransomware Threat Landscape 2023: Ransomware Resurgence, Black Kite provides analysis of 2,708 ransomware victims with insights into attacks from April 2022 to March 2023."

Ransomware Payouts, Lawsuits Rose In 2022, Law Firm Says - Law360

Source: https://www.law360.com/articles/1601753/ransomware-payouts-lawsuits-rose-in-2022-law-firm-says

From the Article: "In the legal profession, information is the key to success. You have to know what's happening with clients, competitors, practice areas, and industries. Law360 provides the intelligence you need to remain an expert and beat the competition."

T-Bones hit by ransomware attack disabling gift card, rewards systems | Local News

Source: https://www.laconiadailysun.com/news/local/t-bones-impacted-by-ransomware-attack-disabling-gift-card-rewards-systems/article_f4dc525c-e532-11ed-8f88-473dec23c677.html

From the Article: "Ransomware is the practice of using hacking techniques to take data hostage."

Ukraine, Western supply chains facing Russian ransomware threats | SC Media

Source: https://www.scmagazine.com/brief/ransomware/ukraine-western-supply-chains-facing-russian-ransomware-threats

From the Article: "While emerging cyber threats and vulnerabilities tend to dominate headlines, criminals often exploit known vulnerabilities to gain access to critical systems and data for nefarious purposes."

The Week in Security: A possible Colonial Pipeline 2.0, ransomware takes bite out of ...

Source: https://securityboulevard.com/2023/04/the-week-in-security-a-possible-colonial-pipeline-2-0-ransomware-takes-bite-out-of-american-eateries/

From the Article: "Welcome to the latest edition of The Week in Security, which brings you the newest headlines from both the world and our team across the full stack of security: application security, cybersecurity, and beyond. This week: A Canada gas pipeline could have suffered an explosion caused by a cyber attack. Also: Financial services firm NCR hit with a ransomware attack, hurting thousands of small American eateries. "

Report: Ransomware group claims to have hacked district court - Audacy

Source: https://www.audacy.com/kywnewsradio/news/national/ransomware-group-claims-to-have-hacked-district-court

From the Article: "A report from The Cyber Express said that a ransomware group called "Everest" claimed to get access to "the network of the US District Court in Illinois, and is now offering to sell that access to interested buyers.""

City of Oakland Restores and Recovers Systems Affected by Ransomware Attack

Source: https://www.oaklandca.gov/news/2023/city-of-oakland-restores-and-recovers-systems-affected-by-ransomware-attack

From the Article: "On February 8, 2023, the City of Oakland experienced a cybersecurity incident, which impacted many of our IT systems. Upon detection, we quickly took steps to contain the threat and secure our network, alerted law enforcement, and launched an investigation. Third-party cybersecurity and forensics experts were engaged to lead the investigation into the scope of the incident."

Malware threat report reveals risk on Mac compared to Windows and Linux - 9to5Mac

Source: https://9to5mac.com/2023/04/27/malware-threat-report-mac-risk-vs-windows-and-linux/

From the Article: "So far this year we've seen a few reports about malware that's affecting Macs. Now Elastic Security Labs has released its spring 2023 Global Threat Report. It offers a big-picture look at the state of malware including how often it's impacting Mac vs Windows and Linux, the most common malware overall, the most common malware on Mac, and more."

Link back to Table of Contents

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

How To Restore Your Financial Data After A Ransomware Attack - Finance Monthly

Source: https://www.finance-monthly.com/2023/04/how-to-restore-your-financial-data-after-a-ransomware-attack/

From the Article: " The primary concern after a ransomware attack is restoring access to your financial data. It may seem like paying the ransom is an easier solution, but it’s not advisable. There’s no guarantee that you’ll get your data back, and you may be exposing yourself to further attacks."

New coercive tactics used to extort ransomware payments - OODA Loop

Source: https://www.oodaloop.com/cyber/2023/04/27/fin7-hackers-caught-exploiting-recent-veeam-vulnerability/

From the Article: "Guidepoint Security has identified an increase in ransomware attacks during Q1 2023. GRIT’s recent report displayed a 27% increase in public ransomware attacks compared to Q1 2022, particularly prevalent in the manufacturing, technology, finance, education, and healthcare sectors. "

Ransomware Protection Market Size, Share, Growth, Trends, By Product Type, By ... - Digital Journal

Source: https://www.digitaljournal.com/pr/news/coherent-market-insights/ransomware-protection-market-size-share-growth-trends-by-product-type-by-application-by-regional-forecast-2023-2030-kaspersky-lab-malwarebytes-corp-mcafee-inc-

From the Article: "The Ransomware Protection market is a rapidly growing industry that provides a wide range of products and services to consumers and businesses. This research study aims to provide a comprehensive analysis of the market, including market size, trends, drivers, challenges, and opportunities. The report also includes an overview of the key players in the market and their competitive landscape."

Prohibition of ransomware payments could have dire consequences, says AGL

Source: https://www.cybersecurityconnect.com.au/policy/8974-prohibition-of-ransomware-payments-could-have-dire-consequences-says-agl

From the Article: "In its submission to the 2023–2030 Australian cyber security strategy discussion paper, AGL has said that banning ransomware payments, while likely to reduce the number of ransomware attacks, could have dire consequences."

Rubrik's New Partnership and Ransomware Warranty - Australian Cyber Security Magazine

Source: https://australiancybersecuritymagazine.com.au/rubriks-new-partnership-and-ransomware-warranty/

From the Article: "Rubrik and Zscaler have announced a new partnership and technology integration to streamline data protection and compliance and boost cyber resilience."

Halcyon: Cyber Resilience Platform Company Raises $50 Million

Source: https://pulse2.com/halcyon-cyber-resilience-platform-company-raises-50-million/

From the Article: "Cyber resilience platform company Halcyon announced that it has raised a $50 million Series A funding round led by SYN Ventures with additional investment from Dell Technologies Capital, Corner Ventures, and other strategic investors."

Hackers with a Heart: Dreaded LockBit 3.0 Ransomware Group Apologies | Full Story

Source: https://www.timesnownews.com/technology-science/hackers-with-a-heart-dreaded-lockbit-3-0-ransomware-group-apologies-full-story-article-99801599

From the Article: "The group's admin expressed regret, saying, "Please forgive me for allowing the attack on small innocent children, the stolen data has been deleted, to get the decryptor please give me the decryption id. I am very ashamed, but I can not control all partners, anyone can join my affiliate program as well as break the rules, I have blocked this partner.""

Ransomware in the Cloud: How to Identify, Respond and Recover - Security Boulevard

Source: https://securityboulevard.com/2023/04/ransomware-in-the-cloud-how-to-identify-respond-and-recover/

From the Article: "Ransomware attacks have been on the rise in recent years, and the cloud is no exception to this trend. As more and more businesses move their data and operations to the cloud, cyber criminals are finding new ways to exploit vulnerabilities and launch ransomware attacks in the cloud. "

50% of companies fell victim to ransomware in the last year - SecurityBrief Asia

Source: https://securitybrief.com.au/story/50-of-companies-fell-victim-to-ransomware-in-the-last-year

From the Article: "Based on a recent global survey conducted by Fortinet, the report explores the perspectives of cybersecurity leaders on ransomware. It particularly focused on how it impacted their organisations in the last year and their strategies to mitigate an attack."

How ransomware victims can make the best of a bad situation - TechTarget

Source: https://www.techtarget.com/searchsecurity/news/365535797/How-ransomware-victims-can-make-the-best-of-a-bad-situation

From the Article: "An RSA conference speaker offered ways for ransomware victims to leverage negotiations and transactions with threat actors and acquire more than just a data decryption key."

This dangerous new malware also has ransomware capabilities - TechRadar

Source: https://www.techradar.com/news/this-dangerous-new-malware-also-has-ransomware-capabilities

From the Article: "A new Android malware variant has been found that’s capable of hiding from antivirus programs, stealing sensitive data, and even deploying ransomware (opens in new tab) on the infected endpoints. "

NSA cyber director warns of ransomware attacks on Ukraine, Western supply chains

Source: https://therecord.media/russia-ransomware-attacks-logistics-supply-chain-ukraine

From the Article: "Russian hackers are attempting to inject ransomware into Ukraine's logistics supply chain and those of the Western countries that back Kyiv in its fight against Moscow, a senior National Security Agency official said on Wednesday."

The Long-term Impact Of Ransomware Attacks On The Finance Industry - The Coin Republic

Source: https://www.thecoinrepublic.com/2023/04/26/the-long-term-impact-of-ransomware-attacks-on-the-finance-industry/

From the Article: "In the majority of Ransomware attacks, the attackers create so much panic that the financial organizations think it's best to give them the money."

91% of Orgs Expect to Increase Cybersecurity Budgets in Next Year - HealthITSecurity

Source: https://healthitsecurity.com/news/91-of-orgs-expect-to-increase-cybersecurity-budgets-in-next-year

From the Article: "As ransomware continues to impact organizations worldwide, cybersecurity leaders are increasingly recognizing the importance of investing resources into improving their security programs and processes. More than 90 percent of surveyed cybersecurity leaders and decision-makers from a variety of industries reported plans to increase security budgets in the coming year, Fortinet found in its 2023 Global Ransomware Report."

Ransomware attacks on the rise again: Report - Business Insurance | News

Source:
https://www.businessinsurance.com/article/20230426/NEWS06/912357034/Ransomware-attacks-on-the-rise-again-Report,-Black-Kite

From the Article: "Black Kite Research tallied 410 organizations that were ransomware victims in March 2023, compared with 208 in April 2022. The Boston-based cybersecurity ratings service based its report on an analysis of 2,708 victims between April 1, 2022, and March 31, 2023."

Link back to Table of Contents

Understanding Ransomware in 2023: How to Protect Your Clients Against Attacks

Source: https://www.channele2e.com/influencers/understanding-ransomware-in-2023-how-to-protect-your-clients-against-attacks/

From the Article: "Ransomware remains the number one cybersecurity threat for large and medium businesses. But now, even smaller organizations can expect to face ransomware attacks as ransomware-as-a-service (RaaS) becomes more prevalent."

Ransomware Attacks Decreasing? Not So Fast, Black Kite Report Shows - MSSP Alert

Source: https://www.msspalert.com/cybersecurity-news/ransomware-attacks-decreasing-not-so-fast-black-kite-report-shows/

From the Article: "The report offers an analysis of 2,708 ransomware victims for the 12-month period from April 2022 to March 2023. Black Kite said of particular interest was that the number of victims in March nearly doubled from last April and were 1.6 times higher than the peak month in 2022."

Case study: reacting to a ransomware attack | Analysis - Strategic Risk Europe

Source: https://www.strategic-risk-europe.com/home/case-study-reacting-to-a-ransomware-attack/1444409.article

From the Article: "The accounting software solution dedicated to small and medium size companies WinBizz, was affected by a major ransomware attack targeting its cloud solution InfoPro last December."

Cyberespionage TTPs, from Tehran and Beijing. SLP exploitation. Ransomware as an ... - CyberWire

Source: https://thecyberwire.com/newsletters/daily-briefing/12/80

From the Article: "Iran's APT Charming Kitten, sponsored by Tehran's Islamic Revolutionary Guard Corps (IRGC), has been seen using a new strain of malware known as BellaCiao, Bitdefender reported this morning. The group, known also by many names (including Mint Sandstorm, Phosphorus, APT35, and APT42) uses this individually-tailored dropper to deliver payloads from their command-and-control (C2) server. "

Healthcare Industry Facing Increased Malware and Ransomware Threats

Source: https://www.hipaajournal.com/healthcare-industry-facing-increased-malware-and-ransomware-threats/

From the Article: "Ransomware actors continue to target the U.S. healthcare sector, cybercriminals are increasingly using malware to steal data and provide persistent access to healthcare networks, and legitimate penetration tools are being used to mask malicious activity amongst genuine use of these tools by red teams."

US Navy contractor Fincantieri Marine Group suffers a ransomware attack - teiss

Source: https://www.teiss.co.uk/news/us-navy-contractor-fincantieri-marine-group-suffers-a-ransomware-attack-12099

From the Article: "Fincantieri Marine Group (FMG), a subsidiary of Italy-based Fincantieri SpA with shipyards in Marinette, Sturgeon Bay, and Green Bay and 2,300 employees, was hit by a ransomware attack on April 12, disrupting operations throughout the shipyard."

Access management in healthcare: Aligning to NIST 800-66

Source: https://www.healthcareitnews.com/news/access-management-healthcare-aligning-nist-800-66

From the Article: "The Health Insurance Portability and Accountability Act (HIPAA) is often the first thing that comes to mind regarding ensuring patient privacy in healthcare.1 But as ransomware attacks and data breaches against healthcare systems continue, HIPAA safeguards must evolve to protect against growing cybercriminal activity."

Cyber Security Today, April 26, 2023 – New reports on ransomware and cyber attacks

Source: https://www.itworldcanada.com/article/cyber-security-today-april-26-2023-new-reports-on-ransomware-and-cyber-attacks/537586

From the Article: "In analyzing victim organizations over the last 12 months the researchers found these things in common: Poor email configuration, recent leaks of usernames and passwords, publicly-available remote access ports, out-of-date systems and IP addresses with botnet activity."

Rubrik & Zscaler partner to produce double extortion ransomware solution - PCR

Source: https://www.pcr-online.biz/2023/04/26/rubrik-zscaler-partner-to-produce-double-extortion-ransomware-solution/

From the Article: "Rubrik and Zscaler have announced a new partnership and technology integration to streamline data protection and compliance and boost cyber resilience. With this new integration, valuable data security insights are placed in the hands of even more security and compliance teams to strengthen data protection policies that help prevent the loss of critical business data."

Ransomware Payment Ban Puts Pressure on Channel to Do More

Source: https://www.channelfutures.com/emea/ransomware-payment-ban-pressure-channel

From the Article: "It's vital that channel partners help customers be more proactive now that there is a large ransomware payment ban in the UK."

Second ransomware group reported exploiting GoAnywhere security flaw - TechRadar

Source: https://www.techradar.com/news/second-ransomware-group-reported-exploiting-goanywhere-security-flaw

From the Article: "The Clop ransomware group is no longer the only threat actor that successfully leveraged the GoAnywhere MFT vulnerability to target an organization. "

Jackson school gives update on November cyberattack - DataBreaches.net

Source: https://www.databreaches.net/jackson-school-gives-update-on-november-cyberattack/

From the Article: "The November ransomware attack forced Jackson and Hillsdale schools to shut down for days. "

Cyberattackers employ over 500 unique tools in 2022, Sophos report reveals

Source: https://mb.com.ph/2023/4/25/cyberattackers-employ-over-500-unique-tools-in-2022-sophos-report-reveals

From the Article: "Unpatched vulnerabilities and compromised credentials have been identified as key root causes of attacks, while ransomware remains the most common "end game.""

Rubrik & Zscaler Announce Industry's First Double Extortion Ransomware Solution

Source: https://www.scoop.co.nz/stories/BU2304/S00331/rubrik-zscaler-announce-industrys-first-double-extortion-ransomware-solution.htm

From the Article: "First in the cybersecurity industry to offer a ransomware recovery warranty of its kind for qualified customers, Rubrik, the Zero Trust Data Security™ Company, today announced it has increased its Ransomware Recovery Warranty offering from up to $5 million to up to $10 million for recovery-related costs."

New coercive tactics used to extort ransomware payments - Help Net Security

Source: https://www.helpnetsecurity.com/2023/04/26/q1-2023-ransomware-victims/

From the Article: "The increase in reported ransomware victims across Q1 2023 reflects the continued prevalence of ransomware as a worldwide, industry agnostic threat, according to GuidePoint Security."

Strolling through Cyberspace and Hunting for Phishing Sites, (Wed, Apr 26th)

Source: https://isc.sans.edu/diary/rss/29780

From the Article: "From time to time and as much as my limited time permits, I often explore the Internet and my DShield logs to see if I can uncover any interesting artifacts that suggest nefarious behaviour. "

Security Risks of AI

Source: https://www.schneier.com/blog/archives/2023/04/security-risks-of-ai.html

From the Article: "Stanford and Georgetown have a new report on the security risks of AI—particularly adversarial machine learning—based on a workshop they held on the topic."

Hacking Pickleball

Source: https://www.schneier.com/blog/archives/2023/04/hacking-pickleball.html

From the Article: "My latest book, A Hacker's Mind, has a lot of sports stories. Sports are filled with hacks, as players look for every possible advantage that doesn't explicitly break the rules."

Taking a Proactive Approach to Ransomware

Source: https://www.secureworks.com/resources/vd-irs-taking-a-proactive-approach-to-ransomware

From the Article: "In this video interview, hear about the prevalence of ransomware and the proactive steps you can take to avoid becoming the latest victim."

Mind the Gap: Understanding Your Attack Surface & Extending Your Response

Source: https://www.secureworks.com/resources/pc-lets-talk-soc-s02e006

From the Article: "George Anderson, Sr. Product Marketing Manager, discusses XDR and why open security platforms hold the key to the future of XDR."

White hat hackers showed how to take over a European Space Agency satellite

Source: https://securityaffairs.com/145483/hacking/esa-satellite-hack.html

From the Article: "This week, during the third edition of CYSAT, the European event dedicated to cybersecurity for the space industry, the European Space Agency (ESA) set up a satellite test bench, inviting white hat hackers to attempt seizing control of OPS-SAT, a nanosatellite operated by the agency for demonstration purposes."

Crooks broke into AT&T email accounts to empty their cryptocurrency wallets

Source: https://securityaffairs.com/145508/hacking/att-email-accounts-hacked.html

From the Article: "Hackers are breaking into the AT&T email accounts and then using the access they are logging into the victim's cryptocurrency exchange accounts to drain their crypto funds, TechCrunch reported."

China-linked Alloy Taurus APT uses a Linux variant of PingPull malware

Source: https://securityaffairs.com/145335/apt/alloy-taurus-apt-pingpull-linux-variant.html

From the Article: "Researchers from Palo Alto Networks Unit 42 recently observed the China-linked Alloy Taurus group (aka GALLIUM, Softcell) targeting Linux systems with a new variant of PingPull backdoor. While investigating the activity of the group, the researchers also identified a previously undocumented backdoor used by the threat actor and tracked as Sword2033."

Thousands of publicly-exposed Apache Superset installs exposed to RCE attacks

Source: https://securityaffairs.com/145317/hacking/superset-flaw.html

From the Article: "Apache Superset is an open-source data visualization and data exploration platform. The maintainers of the software have released security patches to address an insecure default configuration, tracked as CVE-2023-27524 (CVSS score: 8.9), that could lead to remote code execution."

Pro-Russia hacking group executed a disruptive attack against a Canadian gas pipeline

Source: https://securityaffairs.com/145307/cyber-warfare-2/canadian-gas-pipeline-disruptive-attack.html

From the Article: "A Canadian gas pipeline suffered a cyber security incident, Canada's top cyber official and Pro-Russia hacking group Zarya claimed the attack could have caused an explosion."

Innovation Sandbox: Cybersecurity Investors Pivot to Safeguarding AI Training Models

Source: https://www.securityweek.com/innovation-sandbox-cybersecurity-investors-pivot-to-safeguarding-ai-training-models/

From the Article: "SecurityWeek editor-at-large Ryan Naraine expects to see an explosion of well capitalized startups promising to protect AI machine learning models behind enterprise products."

Russian APT Hacked Tajikistani Carrier to Spy on Government, Public Services

Source: https://www.securityweek.com/russian-apt-hacked-tajikistani-carrier-to-spy-on-government-public-services/

From the Article: "Russian espionage group Nomadic Octopus infiltrated a Tajikistani telecoms provider to spy on 18 entities, including government officials and public service infrastructures."

RSA Conference 2023 – ICS/OT Cybersecurity Roundup

Source: https://www.securityweek.com/rsa-conference-2023-ics-ot-cybersecurity-roundup/

From the Article: "SecurityWeek is providing a summary of ICS/OT cybersecurity announcements made at RSA Conference 2023, including talks, products, and new initiatives."

Chinese Cyberspies Delivered Malware via Legitimate Software Updates

Source: https://www.securityweek.com/chinese-cyberspies-delivered-malware-via-legitimate-software-updates/

From the Article: "Chinese APT Evasive Panda has been observed targeting local members of an international NGO with the MgBot backdoor, delivered via legitimate software updates."

Apiiro Launches Application Attack Surface Exploration Tool

Source: https://www.securityweek.com/apiiro-launches-application-attack-surface-exploration-tool/

From the Article: "Apiiro's Risk Graph Explorer helps security teams to understand their application attack surface."

Purple AI | Empowering Cybersecurity Analysts with AI-Driven Threat Hunting, Analysis & Response

Source: https://www.sentinelone.com/blog/purple-ai-empowering-cybersecurity-analysts-with-ai-driven-threat-hunting-analysis-response/

From the Article: "SentinelOne is delighted to introduce Purple AI, a generative AI dedicated to threat-hunting, analysis and response. Purple AI uses a variety of models both open source and proprietary and aims to increase the organization's efficiency by arming security analysts with an AI engine that can help identify, analyze and mitigate threats using conversational prompts and interactive dialog."

Day 3 From RSAC 2023 | Innovations In Threat Hunting and Risks In the Lens of Regulatory Requirements

Source: https://www.sentinelone.com/blog/day-3-from-rsac-2023/

From the Article: "Beat the midweek blues with a full recap of Day 3 here at this year's RSAC. Catch up on presentations the SentinelOne team is sharing on cybersecurity thought leadership, learn about exclusive demos, and feel like you're part of all the action that's happening in San Fran!"

Link back to Table of Contents

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

Homerun browser hijacker

Source: https://www.2-spyware.com/remove-homerun-browser-hijacker.html

From the Article: "Homerun is a bogus browser extension that changes the main settings to generate revenue Homerun, a browser hijacker aimed at sports fans, can change important settings such as your homepage, new tab address, and search engine."

Cybersecurity Snapshot: RSA Conference Special Edition with All-You-Can-Eat AI and ChatGPT

Source: https://www.tenable.com/blog/cybersecurity-snapshot-rsa-conference-special-edition-with-all-you-can-eat-ai-and-chatgpt

From the Article: "Check out our roundup of what we found most interesting at RSA Conference 2023, where – to no one’s surprise – artificial intelligence captured the spotlight, as the cybersecurity industry grapples with a mixture of ChatGPT-induced fascination and worry. Oh generative AI, it hurts so good!"

IDC Ranks Tenable No. 1 in Worldwide Device Vulnerability Management Market Share for the Fourth Consecutive Year

Source: https://www.tenable.com/blog/idc-ranks-tenable-no-1-in-worldwide-device-vulnerability-management-market-share-for-the

From the Article: "IDC credits Tenable’s success to our strategic acquisition strategy and Tenable One, our Exposure Management Platform, which provides extensive vulnerability coverage for IT infrastructure, web apps, public cloud and identity systems, along with context-driven risk analysis, all in one unified platform."

ETHOS: Bringing the OT Security Community Together for Threat Information Sharing

Source: https://www.tenable.com/blog/ethos-bringing-the-ot-security-community-together-for-threat-information-sharing

From the Article: "Tenable participates in a first-of-its-kind initiative that will aggregate information from several operational technology (OT) security vendors to share emerging threat intelligence with critical infrastructure service providers."

Link back to Table of Contents

The articles have been 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 UN's new cybercrime treaty raises human rights concerns. How China's new counter-espionage law could impact cyber business.

Source: https://thecyberwire.com/newsletters/policy-briefing/5/82

From the Article: "The UN's new cybercrime treaty raises human rights concerns. How China's new counter-espionage law could impact cyber business. DHS moves to codify the Cyber Safety Review Board."

PaperCut exploits. AMOS infostealer traded in C2C markets. Malvertising from Vietnam. Self-attestation. Cyber auxiliaries.

Source: https://thecyberwire.com/newsletters/daily-briefing/12/82

From the Article: "Cl0p and LockBit exploit PaperCut vulnerability in ransomware campaigns. Infostealer traded in the C2C market. All ads are trying to get your money, but some just take it."

Current news of cyber gangland. Cyberespionage hits NGO. Hacktivism, supply chains, and developments in hybrid warfare.

Source: https://thecyberwire.com/newsletters/daily-briefing/12/81

From the Article: "Google targets CryptBot malware infrastructure. FIN7 used CVE-2023-27532 to attack Veeam servers and steal credentials. Ransomware-as-a-service offering threatens Linux systems. Chinese APT group Evasive Panda targets NGOs in China."

Ukraine at D+427: Russian cyberattacks and disinformation before Ukraine's spring offensive.

Source:
https://thecyberwire.com/stories/5928f4b47ca643929516331e6638596b/ukraine-at-d427

From the Article: "As Ukraine completes preparations for its spring offensive, Russia seeks to redress the balance of forces with disinformation and ransomware attacks on logistical chains."

Cyberespionage TTPs, from Tehran and Beijing. SLP exploitation. Ransomware as an international threat. Hacktivist update.

Source: https://thecyberwire.com/newsletters/daily-briefing/12/80

From the Article: "BellaCiao malware, from Iran's IRGC. PingPull, malware used by the Chinese government affiliated Tarus Group. CVE-2023-29552 a critical level Service Location Protocol exploit."

Paperbug Attack: New Politically-Motivated Surveillance Campaign in Tajikistan

Source: https://thehackernews.com/2023/04/paperbug-attack-new-politically.html

From the Article: "A little-known Russian-speaking cyber-espionage group has been linked to a new politically-motivated surveillance campaign targeting high-ranking government officials, telecom services, and public service infrastructures in Tajikistan."

Chinese Hackers Spotted Using Linux Variant of PingPull in Targeted Cyberattacks

Source: https://thehackernews.com/2023/04/chinese-hackers-using-pingpull-linux.html

From the Article: "The Chinese nation-state group dubbed Alloy Taurus is using a Linux variant of a backdoor called PingPull as well as a new undocumented tool codenamed Sword2033."

Chinese Hackers Using MgBot Malware to Target International NGOs in Mainland China

Source: https://thehackernews.com/2023/04/chinese-hackers-using-mgbot-malware-to.html

From the Article: "The advanced persistent threat (APT) group referred to as Evasive Panda has been observed targeting an international non-governmental organization (NGO) in Mainland China with malware delivered via update channels of legitimate applications like Tencent QQ."

Link back to Table of Contents

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

Browser Security Survey: 87% of SaaS Adopters Exposed to Browser-borne Attacks

Source: https://thehackernews.com/2023/04/browser-security-survey-87-of-saas.html

From the Article: "The browser serves as the primary interface between the on-premises environment, the cloud, and the web in the modern enterprise. Therefore, the browser is also exposed to multiple types of cyber threats and operational risks."

Modernizing Vulnerability Management: The Move Toward Exposure Management

Source: https://thehackernews.com/2023/04/modernizing-vulnerability-management.html

From the Article: "Managing vulnerabilities in the constantly evolving technological landscape is a difficult task. Although vulnerabilities emerge regularly, not all vulnerabilities present the same level of risk."

Recent Trends in Internet Threats: Common Industries Impersonated in Phishing Attacks, Web Skimmer Analysis and More

Source: https://unit42.paloaltonetworks.com/internet-threats-late-2022/

From the Article: "We observed and analyzed over 67 million unique malicious URLs, domains and IPs. Our findings include targeted sectors and a case study of a web skimmer."

Chinese Alloy Taurus Updates PingPull Malware

Source: https://unit42.paloaltonetworks.com/alloy-taurus/

From the Article: "A PingPull malware variant for Linux has been found. We're also tracking a new backdoor attributed to Alloy Taurus called Sword2033."

Introducing VirusTotal Code Insight: Empowering threat analysis with generative AI

Link back to Table of Contents

Source: https://blog.virustotal.com/2023/04/introducing-virustotal-code-insight.html

From the Article: "At the RSA Conference 2023 today, we are excited to unveil VirusTotal Code Insight, a cutting-edge feature that leverages artificial intelligence for code analysis. Powered by Google Cloud Security AI Workbench, Code Insight produces natural language summaries of code snippets with ease."

Evasive Panda APT group delivers malware via updates for popular Chinese software

Source: https://www.welivesecurity.com/2023/04/26/evasive-panda-apt-group-malware-updates-popular-chinese-software/

From the Article: "ESET Research uncovers a campaign by the APT group known as Evasive Panda targeting an international NGO in China with malware delivered through updates of popular Chinese software."

Subscription Required

Chip designer Arm makes its own advanced prototype semiconductor

Source: https://www.ft.com/content/72897dde-2d84-48b1-8bd7-390e66049d40

From the Article: "Company to build test chip with factory partners, stoking fears it could in future compete with its biggest customers”

China Building Cyberweapons To Hijack Enemy Satellites, Says US Leak

Source: https://www.ft.com/content/881c941a-c46f-4a40-b8d8-9e5c8a6775ba

From the Article: "China is building sophisticated cyber weapons to “seize control” of enemy satellites, rendering them useless for data signals or surveillance during wartime, according to a leaked US intelligence report."

The U.S. Military Relies on One Louisiana Factory. It Blew Up.

Source: https://www.wsj.com/articles/the-u-s-military-has-an-explosive-problem-6e1a1049?mod=hp_lead_pos7

Link back to Table of Contents

The articles have been 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: "Decades of consolidation have left the Pentagon vulnerable to mishaps—including when the sole maker of a crucial type of gunpowder went offline"

'Double Tax' Hinders Taiwan's Investment in American Factories

Source: https://www.wsj.com/articles/double-tax-hinders-taiwans-investment-in-american-factories-db67ec49?mod=Searchresults_pos1&page=1

From the Article: "Taiwan businesses are rushing to produce semiconductor chips in the U.S., but the lack of a formal tax treaty gives investors pause"

Top Biden Aide Says U.S. Subsidies Will Help, Not Hurt, Relationships With Allies

Source: https://www.wsj.com/articles/top-biden-aide-says-u-s-subsidies-will-help-not-hurt-relationships-with-allies-78a4ac7a?mod=Searchresults_pos2&page=1

From the Article: "Close allies in Europe and Asia have said the administration's industrial subsidies are unfair"

Honda to Launch EV in North America in 2025

Source: https://www.wsj.com/articles/honda-to-launch-ev-in-north-america-in-2025-8af55725?mod=Searchresults_pos3&page=1

From the Article: "Honda said it will partner with Taiwan Semiconductor Manufacturing Co. to ensure stable supply of chips for cars"

Memory-Chip Makers Say Recovery Is in Sight After Long Slump

Source: https://www.wsj.com/articles/memory-chip-makers-say-recovery-is-in-sight-after-long-slump-f35a576?mod=Searchresults_pos4&page=1

From the Article: "As losses from downturn run into billions, Samsung and SK Hynix say the market may be bottoming out after production cuts reduce inventories"

Link back to Table of Contents

Beijing's Bain Raid, Espionage Law Are Self-Sabotage

Source: https://www.wsj.com/articles/beijings-bain-raid-espionage-law-are-self-sabotage-40f87276?mod=Searchresults_pos5&page=1

From the Article: "China's economy is bouncing back. Recent moves show that the potential for state overreach is, too."

Intel Faces a Long Climb Back from the Bottom

Source: https://www.wsj.com/articles/intel-faces-a-long-climb-back-from-the-bottom-284d9599?mod=Searchresults_pos6&page=1

From the Article: "Downtrodden stock jumps on better-than-feared results, but lots of work lies ahead"

China Ratchets Up Pressure on Foreign Companies

Source: https://www.wsj.com/articles/china-ratchets-up-pressure-on-foreign-companies-524b958e?mod=Searchresults_pos10&page=1

From the Article: "Detentions, raids and unexpected visits belie Beijing's invitation to overseas investors"

AI's Effects on Cybersecurity Concern U.S. Officials

Source: https://www.wsj.com/articles/u-s-officials-raise-concerns-about-ais-cybersecurity-implications-f32496ed?mod=Searchresults_pos11&page=1

From the Article: "Rush to deploy ChatGPT and other models may leave organizations open to unknown threats, hacks, cybersecurity officials say"

Investors Continue to Back Logistics Tech

Source: https://www.wsj.com/articles/investors-continue-to-back-logistics-tech-97063b1a?mod=Searchresults_pos14&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: "Startups that are invested in robotic arms, visibility software and 3-D printing for chip making are being funded"

Intel Records Its Worst Quarterly Loss Amid PC Slump, Fierce Competition

Source: https://www.wsj.com/articles/intel-corp-intc-q1-earnings-report-2023-91aab8b3?mod=Searchresults_pos15&page=1

From the Article: "Chip maker is cutting costs while pursuing a pricey turnaround effort"

Nearshoring Shift Brings Production Hurdles Closer to Home

Source: https://www.wsj.com/articles/nearshoring-shift-brings-production-hurdles-closer-to-home-6fc418ee?mod=Searchresults_pos16&page=1

From the Article: "Moving facilities to Mexico or other locations near the U.S. raises questions over costs, supplier networks and logistics, companies say"

China Cracks Down on Foreign Businesses - What's News - WSJ Podcasts

Source: https://www.wsj.com/podcasts/whats-news/china-cracks-down-on-foreign-businesses/c40f1e07-0742-4880-b6ce-8efc89bf4768?mod=Searchresults_pos18&page=1

From the Article: "A.M. Edition for April 28. Raids, detentions and unexpected visits to corporate offices by Chinese authorities are undercutting Beijing's message that it's open for business to global investors. Plus, WSJ editor Jason Dean discusses the big takeaways from this week's tech earnings. And Europe narrowly avoids recession as Germany's economic engine falters. Luke Vargas hosts."

Employers Trying New Ways To Push Workers Back To The Office - Your Money Briefing - WSJ Podcasts

Source: https://www.wsj.com/podcasts/your-money-matters/employers-trying-new-ways-to-push-workers-back-to-the-office/dccd9be0-46da-4fb1-a33f-7a5cf5f27803?mod=Searchresults_pos2&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: "Bosses have tried many different tactics to get employees back into the office. Nationally, a number of offices remain sparsely populated, particularly on Mondays and Fridays. WSJ reporter Chip Cutter joins guest host Mohsin Ali to discuss how one company is tying pay to attendance."

Biden Seeks Seoul's Pledges on Ukraine, Nuclear Deterrence

Source: https://www.wsj.com/articles/biden-seeks-seouls-pledge-to-send-arms-to-ukraine-e4c2af48?mod=Searchresults_pos8&page=1

From the Article: "Intelligence leak and trade are expected on the agenda in state visit from South Korea's President Yoon"

U.S. Struggles to Replenish Munitions Stockpiles as Ukraine War Drags On

Source: https://www.wsj.com/articles/u-s-push-to-restock-howitzer-shells-rockets-sent-to-ukraine-bogs-down-f604511a?mod=Searchresults_pos12&page=1

From the Article: "Supplies are drained at the same time Pentagon, defense industry look to deter China"

How 5G Could Make Virtual-Reality Devices Better

Source: https://www.wsj.com/articles/5g-virtual-reality-benefits-df58f6c4?mod=Searchresults_pos15&page=1

From the Article: "VR headsets and AR glasses have largely been limited to home and office settings. The hope is that 5G will let them be used on the go."

Big Tech Earnings Spark Hope That Worst Is Over

Source: https://www.wsj.com/articles/big-tech-earnings-spark-hope-that-worst-is-over-c672c5d7?mod=Searchresults_pos17&page=1

From the Article: "Shares rise on better-than-expected results, but growth lags behind what Microsoft, Amazon and Google did in past"

Link back to Table of Contents

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

Tesla's Price Cuts Slow a Rival in the Race to Deliver Self-Driving Tech

Source: https://www.wsj.com/livecoverage/stock-market-today-dow-jones-04-27-2023/card/tesla-s-price-cuts-slow-a-rival-in-the-race-to-deliver-self-driving-tech-pO1vq8GciuAVLeQdmojo?mod=Searchresults_pos19&page=1

From the Article: "Six months ago, Tesla started cutting prices in China. That same week, shares of rival self-driving technology provider Mobileye surged on their first day of trading following a hotly anticipated IPO. Now Tesla's price war is catching up with one of its most ambitious competitors in the race to automate driving."

AI's Effects on Cybersecurity Concern U.S. Officials

Source: https://www.wsj.com/articles/u-s-officials-raise-concerns-about-ais-cybersecurity-implications-f32496ed?mod=Searchresults_pos2&page=2

From the Article: "Rush to deploy ChatGPT and other models may leave organizations open to unknown threats, hacks, cybersecurity officials say"

UPS CFO Looks to Speed Up Some Cost Cuts as Shipping Volumes Fall

Source: https://www.wsj.com/articles/ups-cfo-looks-to-speed-up-some-cost-cuts-as-shipping-volumes-fall-922e6cdd?mod=Searchresults_pos6&page=2

From the Article: "The delivery giant said it would finish setting up new technology in more than 900 U.S. buildings by October, two months earlier than planned"

Chinese Warships and Planes Test Taiwan Defenses

Source: https://www.wsj.com/articles/chinese-combat-drone-circles-taiwan-in-mass-incursion-44116201?mod=Searchresults_pos7&page=2

From the Article: "PLA combat drone circles self-governing island amid tensions between Beijing and Taipei"

In China, a Detention and a New Espionage Law Have Businesses Worried

Link back to Table of Contents

Source: https://www.wsj.com/articles/in-china-a-detention-and-a-new-espionage-law-have-businesses-worried-78fc88b1?mod=Searchresults_pos20&page=2

From the Article: "Executives say activity could stagnate as they curtail meetings and information exchange"

Amazon Rebounds From Postpandemic Doldrums, but Says Cloud Growth Is Slowing

Source: https://www.wsj.com/articles/amazon-amzn-q1-earnings-report-2023-cb206c2a?mod=Searchresults_pos8&page=3

From the Article: "Other large tech companies this week saw shares jump after modestly beating Wall Street projections"

Weapons Makers Can’t Hire Enough Workers as Ukraine War Drives Demand

Source: https://www.wsj.com/articles/weapons-makers-cant-hire-enough-workers-as-ukraine-war-drives-demand-d1b74bee?mod=Searchresults_pos10&page=3

From the Article: "Rising geopolitical tensions have boosted military spending, prompting an industrywide hiring spree"

Telecom Companies Pin 5G Hopes on Private Industrial Networks

Source: https://www.wsj.com/articles/5g-companies-industrial-networks-fe0561d4?mod=Searchresults_pos12&page=3

From the Article: "The companies believe that the benefits to manufacturers, mining companies and others are easier to grasp than in the consumer market"

The Debt Ceiling Fight Begins - The Journal. - WSJ Podcasts

Source: https://www.wsj.com/podcasts/the-journal/the-debt-ceiling-fight-begins/57e6e4f4-9055-4e81-a188-26ab1337834e?mod=Searchresults_pos17&page=3

From the Article: "The U.S. only has a few months until it can no longer pay its bills. Republicans say they’ll only raise the debt ceiling if Democrats agree to aggressive spending cuts. WSJ’s Natalie Andrews explains the Republican proposal and what’s at stake for the economy."

A Debt-Ceiling Victory for Kevin McCarthy, but Joe Biden Won't Negotiate - Opinion: Potomac Watch - WSJ Podcasts

Source: https://www.wsj.com/podcasts/opinion-potomac-watch/a-debt-ceiling-victory-for-kevin-mccarthy-but-joe-biden-wont-negotiate/e580dba1-2b41-458c-a76c-f12b82c07ea8?mod=Searchresults_pos20&page=3

From the Article: "Speaker of the House Kevin McCarthy kept Republicans together in the House as the bill raising the debt ceiling was passed and now heads to the Senate. But how will Mitch McConnell and Chuck Schumer handle getting it to the President's desk, despite Joe Biden stating he will not negotiate with the Speaker? Plus, a disappointing report on first-quarter GDP growth points to an economic slowdown and a possible recession. "

CFOs Focus on Building Resilient Supply Chains, Even as Pandemic Disruptions Fade

Source: https://www.wsj.com/articles/cfos-focus-on-building-resilient-supply-chains-even-as-pandemic-disruptions-fade-8192831f?mod=Searchresults_pos1&page=1

From the Article: "Finance executives boost automation and diversify sourcing. ‘I’m diving into the details more,’ says one CFO."

Here’s How Supply Chains Are Being Reshaped for a New Era of Global Trade

Source: https://www.wsj.com/articles/supply-chains-have-changed-forever-819d9afd?mod=Searchresults_pos2&page=1

From the Article: "Nearshoring. Automation. Supplier diversification. Sustainability. Companies are adapting their operations to changing market pressures and geopolitics."

The U.S. Wants a Rare-Earths Supply Chain. Here’s Why It Won’t Come Easily.

Source: https://www.wsj.com/articles/the-u-s-wants-a-rare-earths-supply-chain-hereswhy-it-wont-come-easily-dfc3b632?mod=Searchresults_pos3&page=1

From the Article: "New tax credit bill seeks to challenge China's dominance in the processing of critical minerals"

SEC's Climate-Disclosure Rule Isn't Here, but It May as Well Be, Many Businesses Say

Source: https://www.wsj.com/articles/secs-climate-disclosure-rule-isnt-here-but-it-may-as-well-be-many-businesses-say-854789bd?mod=Searchresults_pos4&page=1

From the Article: "Legal challenges to the regulator's proposed mandate for emissions tracking are all but certain, but many companies see value in assessing their suppliers even if so-called Scope 3 rules get watered down"

Climate-Disclosure Rules Are Coming. Here's How Companies Are Adapting.

Source: https://www.wsj.com/articles/climate-disclosure-rules-are-coming-heres-how-companies-are-adapting-2973200c?mod=Searchresults_pos7&page=1

From the Article: "Corporate efforts to prepare for Scope 3 supply-chain requirements often involve partnerships inside and across industries"

A Cyberattack Forced a Logistics Company to Temporarily Halt Operations

Source: https://www.wsj.com/articles/a-cyberattack-forced-a-logistics-company-to-temporarily-halt-operations-dde27a19?mod=Searchresults_pos10&page=1

From the Article: "A breach at Expeditors International contributed to supply-chain snarls in 2022"

WSJ News Exclusive | China's Dominance Over U.S. Solar Market Grows Despite Efforts to Stem It

Source: https://www.wsj.com/articles/china-dominates-u-s-solar-market-as-lawmakers-tussle-over-tariffs-7c2d749d?mod=Searchresults_pos13&page=1

From the Article: "Chinese market share expected to rise even as Congress debates tariffs to limit it"

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_pos14&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"

Europe’s Green-Energy Push Struggles to Match U.S. Momentum

Source: https://www.wsj.com/articles/europe-clean-energy-renewables-us-4ce5d3e1?mod=Searchresults_pos16&page=1

From the Article: "U.S. tax credits for renewable-energy projects draw investment from across the Atlantic"

Truck Drivers Bear Big Burden on Data Collection. Some Companies Want to Change That.

Source: https://www.wsj.com/articles/truck-drivers-bear-big-burden-on-data-collection-some-companies-want-to-change-that-37fe8324?mod=Searchresults_pos6&page=2

From the Article: "Estes Express Lines is looking to automate more data collection and streamline data sharing to reduce the burden on truckers and dockworkers to track goods"

Ocean Container Lines Push a Rebound in Trans-Pacific Shipping Prices

Source: https://www.wsj.com/articles/ocean-container-lines-push-a-rebound-in-trans-pacific-shipping-prices-a6a85fe3?mod=Searchresults_pos7&page=2

From the Article: "A jump in rates is adding urgency, and higher costs, to planning for the peak importing season"

Link back to Table of Contents

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

Russian Shipbuilders Are Running Out of Parts

Source: https://www.wsj.com/articles/russian-shipbuilders-are-running-out-of-parts-389c2c60?mod=Searchresults_pos8&page=2

From the Article: "Biggest Russian shipyards struggle to find enough propellers and engine parts"

Kerogen Capital-Formed CelerateX Targets $1 Billion for Clean Energy

Source: https://www.wsj.com/articles/kerogen-capital-formed-celeratex-targets-1-billion-for-clean-energy-f3ee13a1?mod=Searchresults_pos12&page=2

From the Article: "The recently established platform invests in less-popular segments such as geothermal energy and hydrogen fuels"

GDP Report Shows Economic Growth Slowed in First Quarter

Source: https://www.wsj.com/articles/us-gdp-economic-growth-first-quarter-2023-2ff4348c?mod=Searchresults_pos18&page=2

From the Article: "Many economists are predicting a U.S. recession later this year"

Kremlin Extends Global Influence With Russian Nuclear-Power Juggernaut

Source: https://www.wsj.com/articles/kremlin-extends-global-influence-with-russian-nuclear-power-juggernaut-d26379a0?mod=Searchresults_pos19&page=2

From the Article: "Russia’s atomic-energy giant Rosatom does business around the world, including with the U.S. and allies like Turkey"

GM Raises 2023 Profit Outlook, Kills Off Chevy Bolt EV

Source: https://www.wsj.com/articles/general-motors-gm-q1-earnings-report-2023-cbebcafc?mod=Searchresults_pos2&page=3

From the Article: "The auto maker’s upbeat forecast defies predictions that the industry’s pricing power will run out of gas"

Look Out, Tesla, There’s a Really Tiny Competitor in Your Rearview Mirror

Source: https://www.wsj.com/articles/electric-vehicle-tiny-bolivia-86b28ebf?mod=Searchresults_pos5&page=3

From the Article: "An electric vehicle made in Bolivia has a top speed of 35 mph and fits three people, ‘but they can’t be very fat’"

WSJ News Exclusive | Companies Are Colluding to Cheat H-1B Visa Lottery, U.S. Says

Source: https://www.wsj.com/articles/u-s-says-some-companies-cheat-h-1b-lottery-driving-record-applications-1a3e4fd?mod=Searchresults_pos13&page=3

From the Article: "Multiple employers are said to enter same applicants to boost chances"

Europe Moves Toward Cutting a Last Source of Russian Energy

Source: https://www.wsj.com/articles/europe-moves-toward-cutting-a-last-source-of-russian-energy-2caf3859?mod=Searchresults_pos16&page=3

From the Article: "Steps to limit shipments of LNG from Russia could push up natural-gas prices"

China’s Oil Strategy Mixes Diplomacy and a Domestic Drilling Push

Source: https://www.wsj.com/articles/chinas-oil-strategy-mixes-diplomacy-and-a-domestic-drilling-push-89a1cedf?mod=Searchresults_pos5&page=4

From the Article: "Newly discovered domestic sources of oil add to supply from sanctioned nations"

China Celebrates Economic Recovery, Pledges More Help on Jobs

Source: https://www.wsj.com/articles/china-celebrates-economic-recovery-pledges-more-help-on-jobs-913398cb?mod=Searchresults_pos8&page=4

From the Article: "Communist Party’s top policy-making body acknowledges concerns about consumer demand"

U.S., South Korea Nuclear Pledge Follows North Korean Weapons Advances

Source: https://www.wsj.com/articles/u-s-south-korea-nuclear-pledge-follows-north-korean-weapons-advances-eb593d7?mod=Searchresults_pos10&page=4

From the Article: "Kim Jong Un’s regime has poured its resources into developing a more capable atomic arsenal"

Russia Renews Threats to Black Sea Grain Deal

Source: https://www.wsj.com/articles/russia-strikes-history-museum-in-recaptured-ukrainian-city-28746610?mod=Searchresults_pos20&page=4

From the Article: "Moscow accuses Ukraine of violating agreement with attacks in Crimea"

Sliding Diesel Prices Signal Warning for U.S. Economy

Source: https://www.wsj.com/articles/sliding-diesel-prices-signal-warning-for-u-s-economy-c6400724?mod=Searchresults_pos1&page=5

From the Article: "‘Freight recession’ means fewer trucks carrying goods across the country"

Auto-Parts Growth Story Still Adds Up

Source: https://www.wsj.com/articles/auto-parts-growth-story-still-adds-up-c5a6471c?mod=Searchresults_pos11&page=5

From the Article: "Fundamentals still look strong for auto-parts retail"

Link back to Table of Contents

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

Opinion | Forget AI: The Administrative State Is a Bad Algorithm

Source: https://www.wsj.com/articles/forget-ai-the-administrative-state-is-a-bad-algorithm-microsoft-ftc-ethylene-oxide-chicago-355dc0a4?mod=Searchresults_pos10&page=6

From the Article: "Microsoft trustbusters and EPA regulators show chatbots aren't the only ones who 'hallucinate.'"

Europe's Economy Barely Avoids Recession

Source: https://www.wsj.com/articles/europes-economy-avoids-recessionjust-about-77e56ab4?mod=Searchresults_pos11&page=6

From the Article: "Rise in factory output, falling energy costs help drive modest rebound"

Russian Oil Prices Surge, Put Sanctions to Test - The Wall Street Journal Google Your News Update - WSJ Podcasts

Source: https://www.wsj.com/podcasts/google-news-update/russian-oil-prices-surge-put-sanctions-to-test/a5e931ba-12be-478c-b8cb-68defb50d7d2?mod=Searchresults_pos18&page=6

From the Article: "Urals crude has bubbled from a low of $35 a barrel in January to close to the $60-a-barrel limit the U.S. and allies placed on most Russian crude exports. Wall Street Journal reporter Joe Wallace joins WSJ What's News host Luke Vargas to explain why those price rises are putting pressure on the West's ability to keep Russian oil on the market while still pinching the Kremlin's revenue. "

Banking Problems May Be Tip of Debt Iceberg

Source: https://www.wsj.com/articles/banking-problems-may-be-tip-of-debt-iceberg-262b6d0e?mod=Searchresults_pos4&page=7

From the Article: "'Shadow banks' have grown rapidly and, like banks, are exposed to risk from higher interest rates"

Link back to Table of Contents

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

China’s Xi Seeks to Regain Initiative in Europe Through Ukraine

Source: https://www.wsj.com/articles/chinas-xi-seeks-to-regain-initiative-in-europe-through-ukraine-23f3618b?mod=Searchresults_pos5&page=7

From the Article: "Dialogue with Ukrainian President Zelensky follows weeks of intense European diplomacy"

Republicans Pass Debt-Ceiling Bill Aiming to Spark Talks With Biden - What’s News - WSJ Podcasts

Source: https://www.wsj.com/podcasts/whats-news/republicans-pass-debt-ceiling-bill-aiming-to-spark-talks-with-biden/48e4630d-f2c4-4c7d-a94b-34a633c4e0b8?mod=Searchresults_pos12&page=7

From the Article: "P.M. Edition for April 26. House Republicans advance a bill to raise the debt ceiling. Plus, a U.K. watchdog has rejected Microsoft’s $75 billion deal for videogame maker Activision Blizzard, complicating its prospects. Reporter Kim Mackrael has more. Annmarie Fertoli hosts. "

Evolution Equity Partners Builds on Cybersecurity Opportunities

Source: https://www.wsj.com/articles/evolution-equity-partners-builds-on-cybersecurity-opportunities-f28b716e?mod=Searchresults_pos1&page=1

From the Article: "The specialist startup investor expects unsettled markets to spur more digital attacks, driving demand for protection against hacks and hackers"

U.S. Cyber Plans Are Built to Endure Political Winds, Senior Security Official Says

Source: https://www.wsj.com/articles/u-s-cyber-plans-are-built-to-endure-political-winds-senior-security-official-says-ab240d3f?mod=Searchresults_pos3&page=1

From the Article: "Kemba Walden, acting national cyber director, said broad bipartisan agreement means national cybersecurity agenda will survive administrations"

Link back to Table of Contents

The articles have been 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’s Eric Goldstein on Bridging Public-Private Cyber Gaps

Source: https://www.wsj.com/articles/cisas-eric-goldstein-on-bridging-public-private-cyber-gaps-e8d36861?mod=Searchresults_pos5&page=1

From the Article: "Senior official at the U.S. Cybersecurity and Infrastructure Security Agency discusses the challenges of working with the government and industry"

Google Debuts Cybersecurity-Focused AI System

Source: https://www.wsj.com/articles/google-debuts-cybersecurity-focused-ai-system-33a24f8e?mod=Searchresults_pos6&page=1

From the Article: "Platform combines generative AI with threat intelligence for cyber analysts"

U.S. Sent Teams into Foreign Networks to Hunt SolarWinds, Microsoft Hackers

Source: https://www.wsj.com/articles/u-s-sent-teams-into-foreign-networks-to-hunt-solarwinds-microsoft-hackers-f71341f3?mod=Searchresults_pos7&page=1

From the Article: "Mixed military-civilian cyber team spied on SolarWinds attackers, filched malware used against Microsoft email product"

Cyber Chiefs Forge Partnerships With Physical Security Units as Combined Threats Grow

Source: https://www.wsj.com/articles/cyber-chiefs-forge-partnerships-with-physical-security-units-as-combined-threats-grow-56eedf5f?mod=Searchresults_pos8&page=1

From the Article: "AI can help identify potential cyber-physical attacks, says Schneider Electric CIO Elizabeth Hackenson"

Corporate Technology Under New Scrutiny Amid Recession Fears

Source: https://www.wsj.com/articles/corporate-technology-under-new-scrutiny-amid-recession-fears-a69c6583?mod=Searchresults_pos10&page=1

From the Article: "CIOs face pressure from financial chiefs and boards to streamline spending on software and cloud and re-evaluate talent strategies"

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_pos13&page=1

From the Article: "New U.S. government report warns inconsistent vetting procedures, backlogs are among factors that hobble security-clearance system"

Ballooning Software Prices Complicate Tech Spending

Source: https://www.wsj.com/articles/ballooning-software-prices-complicate-tech-spending-calculus-for-cios-f6b3bf92?mod=Searchresults_pos14&page=1

From the Article: "Price hikes as steep as 30% are leading some CIOs to consider switching tech vendors. ‘But it’s very hard to get a divorce,’ one CIO comments"

U.S. is concerned about rivals’ space threats, leaked documents show

Source: https://www.washingtonpost.com/technology/2023/04/25/space-warfare-leaked-documents/

From the Article: "Russia’s troubled space program “very likely will diminish during the next decade” as it faces increased global competition, U.S. sanctions and the rise of SpaceX, which has eaten a large chunk of Russia’s space launch revenue, according to a leaked top secret U.S. intelligence document obtained by The Washington Post. At the same time, China has developed significant capabilities “to hold key U.S. and Allied space assets at risk,” and would deploy them in any conflict with Taiwan, according to another leaked document."

Japan to give chipmaker Rapidus nearly $2bn more in aid

Source: https://asia.nikkei.com/Business/Tech/Semiconductors/Japan-to-give-chipmaker-Rapidus-nearly-2bn-more-in-aid

Link back to Table of Contents

The articles have been 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: "Money going to R&D, including dispatching of engineers to IBM"

G-7 ministers agree to 'five principles' for assessing AI risks

Source: https://asia.nikkei.com/Business/Technology/G-7-ministers-agree-to-five-principles-for-assessing-AI-risks

From the Article: "TOKYO -- The Group of Seven leading industrialized nations will call for the creation of international standards for assessing the risks associated with generative artificial intelligence at the digital and technology ministers meeting that opened Saturday to promote the technology's prudent development."

U.S. considers landing bombers in South Korea: Air Force general

Source: https://asia.nikkei.com/Politics/Defense/U.S.-considers-landing-bombers-in-South-Korea-Air-Force-general

From the Article: "Wilsbach eyes trilateral drills with Seoul, Tokyo to address Pyongyang provocations"

Yoon-Biden summit disappoints corporate South Korea

Source: https://asia.nikkei.com/Politics/International-relations/Biden-s-Asia-policy/Yoon-Biden-summit-disappoints-corporate-South-Korea

From the Article: "U.S. makes no visible concessions for chipmakers Samsung, SK Hynix"

Banning generative AI is not an option for Germany: minister

Source: https://asia.nikkei.com/Spotlight/G-7-in-Japan/Banning-generative-AI-is-not-an-option-for-Germany-minister2

From the Article: "European digital ministers at G-7 meet back use after Italy bans ChatGPT"

Link back to Table of Contents

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

Japan wins G-7 support for 'avoided emissions' climate concept

Source: https://asia.nikkei.com/Spotlight/Environment/Climate-Change/Japan-wins-G-7-support-for-avoided-emissions-climate-concept

From the Article: "Expert says guidelines help but are no substitute for cutting greenhouse gases"

G-7 farm ministers condemn Russia for war's impact on food security

Source: https://asia.nikkei.com/Politics/Ukraine-war/G-7-farm-ministers-condemn-Russia-for-war-s-impact-on-food-security

From the Article: "MIYAZAKI, Japan (Kyodo) -- The Group of Seven farm ministers on Sunday condemned Russia for its war against Ukraine and the impact the conflict has had on global food security while also agreeing to help Kyiv revive its agriculture industry by sharing knowledge on demining farmland and rebuilding infrastructure. "

Honda, others to receive $1.8bn in battery, semiconductor subsidies

Source: https://asia.nikkei.com/Politics/Honda-others-to-receive-1.8bn-in-battery-semiconductor-subsidies

From the Article: "Japan supports domestic production of critical items, including EV parts"

Taiwan GDP down 3.02% in Q1 as economy sinks into recession

Source: https://asia.nikkei.com/Economy/Taiwan-GDP-down-3.02-in-Q1-as-economy-sinks-into-recession

From the Article: "Preliminary data disappoints amid sluggish demand for tech exports"

Microsoft cuts production of Surface accessories amid PC slump

Source: https://asia.nikkei.com/Spotlight/Supply-Chain/Microsoft-cuts-production-of-Surface-accessories-amid-PC-slump

Link back to Table of Contents

The articles have been 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: "Suppliers given short notice as tech giant consolidates resources"

Japan to resume preferential trade status on exports to South Korea

Source: https://asia.nikkei.com/Politics/International-relations/Japan-to-resume-preferential-trade-status-on-exports-to-South-Korea

From the Article: "Tokyo to put Seoul back on its 'Group A' list after 2019 downgrade"

China's expanded espionage law has businesses walking on eggshells

Source: https://asia.nikkei.com/Business/Companies/China-s-expanded-espionage-law-has-businesses-walking-on-eggshells

From the Article: "Experts warn that political discussions, photography could trigger scrutiny"

Microsoft trims hardware output, India seeks new investors

Source: https://asia.nikkei.com/techAsia/Microsoft-trims-hardware-output-India-seeks-new-investors

From the Article: "The inside story on the Asia tech trends that matter, from Nikkei Asia and the Financial Times"

Vietnam readies another sales tax cut to prop up flagging economy

Source: https://asia.nikkei.com/Economy/Vietnam-readies-another-sales-tax-cut-to-prop-up-flagging-economy

From the Article: "Value-added tax to decrease to 8% as weak exports bite"

U.S. to send nuclear ballistic sub to South Korea in show of force

Source: https://asia.nikkei.com/Politics/Defense/U.S.-to-send-nuclear-ballistic-sub-to-South-Korea-in-show-of-force

Link back to Table of Contents

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

From the Article: "Biden and Yoon bolster extended deterrence against Pyongyang's provocations"

Honda Motor taps TSMC to ensure 'stable' supply of chips

Source: https://asia.nikkei.com/Business/Tech/Semiconductors/Honda-Motor-taps-TSMC-to-ensure-stable-supply-of-chips

From the Article: "Strategic partnership comes as automaker steps up EV push"

Vietnam, Taiwan boost share of shipments to U.S. as China loses out

Source: https://asia.nikkei.com/Spotlight/Caixin/Vietnam-Taiwan-boost-share-of-shipments-to-U.S.-as-China-loses-out

From the Article: "India, Cambodia also grow as 'low-cost' exporters, eroding Chinese dominance"

In Biden summit, Yoon to seek chip breaks, support on North Korea

Source: https://asia.nikkei.com/Politics/International-relations/In-Biden-summit-Yoon-to-seek-chip-breaks-support-on-North-Korea

From the Article: "President also under pressure to get answers regarding alleged U.S. spying"

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"

The Tragic Fallout From a School District's Ransomware Breach | WIRED

Link back to Table of Contents

Source: https://www.wired.com/story/minneapolis-public-schools-ransomware-attack/

From the Article: "Ransomware gangs have long sought pain points where their extortion demands have the greatest leverage. Now an investigation from NBC News has made clear what that merciless business model looks like when it targets kids."

A Security Team Is Turning This Malware Gang's Tricks Against It | WIRED

Source: https://www.wired.com/story/gootloader-malware-ip-block/

From the Article: "Certain cybercriminal groups like ransomware gangs, botnet operators, and financial fraud scammers get specific attention for their attacks and operations. But the larger ecosystem that underlies digital crime includes an array of actors and malicious organizations that essentially sell support services to these criminal customers."

Bank Turmoil Seen Crimping Credit at Double Powell's Estimate

Source: https://www.bloomberg.com/news/articles/2023-04-26/bank-turmoil-seen-crimping-credit-at-double-powell-s-estimate??leadSource=uverify%20wall

From the Article: "Most economists see half-point hike impact or more from banks. Consensus sees recession coming, likely this quarter or next."

Link back to Table of Contents

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