Weekly Security Articles 15-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.

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

DMSMS Management Best Practices and Lessons Learned: SD-22 DoD DMSMS Guidebook

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

May 18, 2023

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

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

May 24, 2023

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

Events - In-person

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

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

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

June 5-7, 2023

GS1 Connect

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

June 5-7, 2023

Techno Security & Digital Forensics Conference

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

June 5-8, 2023

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

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

June 5-9, 2023

Vendor & Third Party Risk Europe - Center for Financial Professionals

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

June 12-13, 2023

Auto-ISAC Europe Cybersecurity Summit — Automotive ISAC

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

June 13 -14, 2023

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

Infosecurity Europe 2023

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

June 20-22, 2023

Cyber Week

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

June 26-29, 2023

Symposium on Counterfeit Parts and Materials

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

June 27-29, 2023

.conf22 User Conference | Splunk

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

July 17-20, 2023

Black Hat

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

August 5-10, 2023

CIO Leaders Summit Philippines

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

August 8, 2023

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

DEF CON 31

Source: https://defcon.org/

August 10-13, 2023

2023 PCI North America Community Meeting

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

September 12-14, 2023

Mind The Sec

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

September 12-14, 2023

Critical Infrastructure Protection & Resilience Europe

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

September 26-28, 2023

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

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

September 26-28, 2023

Cloud Expo Asia

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

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

October 11-12, 2023

Les Assises

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

October 11-14, 2023

GITEX

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

October 16-20, 2023

IEEE PAINE Conference

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

October 24-26, 2023

2023 PCI Europe Community Meeting

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

October 24-26

CISO Leaders Summit Thailand

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

November 7, 2023

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

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

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

November 2023

Defense Manufacturing Conference Information

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

December 11-14, 2023

Request for Comments

Manufacturing Supply Chain Traceability Using Blockchain Related Technologies
Source: https://www.nccoe.nist.gov/projects/manufacturing-supply-chain-traceability-using-blockchain-related-technologies

Comments due: May 16, 2023

Draft Standardization Roadmap for Additive Manufacturing Version 3.0 Released for Comment

Source: https://www.ansi.org/news/standards-news/all-news/2023/05/5-1-23-draft-standardization-roadmap-for-additive-manufacturing-version-3-released-for-comment

From the Article: "Request for Comments. COMMENTS INVITED BY MAY 31, 2023"

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

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

Comments Due: June 7, 2023

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

Link back to Table of Contents

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

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

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

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

Patches/Advisories

CISA Releases One Industrial Control Systems Advisory

https://www.cisa.gov/news-events/alerts/2023/05/02/cisa-releases-one-industrial-control-systems-advisory

Mitsubishi Electric Factory Automation Products

https://www.cisa.gov/news-events/ics-advisories/icsa-23-122-01

CISA Urges Organizations to Incorporate the FCC Covered List Into Risk Management Plans

https://www.cisa.gov/news-events/alerts/2023/05/01/cisa-urges-organizations-incorporate-fcc-covered-list-risk-management-plans

Accelerating Our Economy Through Better Security: Helping America's Small

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

Businesses Address Cyber Threats

https://www.cisa.gov/news-events/news/accelerating-our-economy-through-better-security-helping-americas-small-businesses-address-cyber

CVE-2023-28231: RCE in the Microsoft Windows DHCPv6 Service

https://www.thezdi.com/blog/2023/5/1/cve-2023-28231-rce-in-the-microsoft-windows-dhcpv6-service

Review - 1 Advisory Published – 5-2-23

https://chemical-facility-security-news.blogspot.com/2023/05/review-1-advisory-published-5-2-23.html

ESB-2023.2479 - [Appliance] Mitsubishi Electric Factory Automation Products: CVSS (Max): 8.8

https://www.auscert.org.au/bulletins/ESB-2023.2479

CISA Releases One Industrial Control Systems Advisory

https://www.cisa.gov/news-events/alerts/2023/05/04/cisa-releases-one-industrial-control-systems-advisory

Review - 1 Update Published – 5-4-23

https://chemical-facility-security-news.blogspot.com/2023/05/review-1-update-published-5-4-23.html

Intelligence community working with private sector to understand impacts of generative AI

https://defensescoop.com/2023/05/04/intelligence-community-generative-ai/

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

Review – Public ICS Disclosures – Week of 4-29-23

https://chemical-facility-security-news.blogspot.com/2023/05/review-public-ics-disclosures-week-of-4.html

Patches/Advisories Articles of Interest

CVE-2023-25492

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-25492

From the Article: "A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API."

CVE-2023-28092

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-28092

From the Article: "A potential security vulnerability has been identified in HPE ProLiant RL300 Gen11 Server. The vulnerability could result in the system being vulnerable to exploits by attackers with physical access inside the server chassis."

CVE-2023-2235

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-2235

From the Article: "A use-after-free vulnerability in the Linux Kernel Performance Events system can be exploited to achieve local privilege escalation."

CVE-2023-2248

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-2248

Link back to Table of Contents
The articles have been 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 heap out-of-bounds read/write vulnerability in the Linux Kernel traffic control (QoS) subsystem can be exploited to achieve local privilege escalation."

CVE-2023-2565

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-2565

From the Article: "A vulnerability has been found in SourceCodester Multi Language Hotel Management Software 1.0 and classified as problematic. This vulnerability affects unknown code of the file ajax.php of the component POST Parameter Handler."

CVE-2023-31047

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-31047

From the Article: "In Django 3.2 before 3.2.19, 4.x before 4.1.9, and 4.2 before 4.2.1, it was possible to bypass validation when using one form field to upload multiple files. This multiple upload has never been supported by forms.FileField or forms."

CVE-2023-2560

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-2560

From the Article: "A vulnerability was found in jja8 NewBingGoGo up to 2023.5.5.2. It has been rated as problematic. This issue affects some unknown processing. The manipulation leads to cross site scripting."

CVE-2023-29963

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-29963

From the Article: "S-CMS v5.0 was discovered to contain an authenticated remote code execution (RCE) vulnerability via the component /admin/ajax.php."

CVE-2023-30065

Link back to Table of Contents

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-30065

From the Article: "MitraStar GPT-2741GNAC-N2 with firmware BR_g5.9_1.11(WVK.0)b32 was discovered to contain a remote code execution (RCE) vulnerability in the ping function."

CVE-2022-43866

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-43866

From the Article: "IBM Maximo Asset Management 7.6.1.2 and 7.6.1.3 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session."

CVE-2023-28068

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-28068

From the Article: "Dell Command Monitor, versions 10.9 and prior, contains an improper folder permission vulnerability."

CVE-2023-30122

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-30122

From the Article: "An arbitrary file upload vulnerability in the component /admin/ajax.php?action=save_menu of Online Food Ordering System v2.0 allows attackers to execute arbitrary code via uploading a crafted PHP file."

CVE-2023-30135

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-30135

From the Article: "Tenda AC18 v15.03.05.19(6318_)_cn was discovered to contain a command injection vulnerability via the deviceName parameter in the setUsbUnload function."

Link back to Table of Contents

CVE-2017-20183

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-20183

From the Article: "A vulnerability was found in External Media without Import Plugin up to 1.0.0 on WordPress. It has been declared as problematic. This vulnerability affects the function print_media_new_panel of the file external-media-without-import.php. The manipulation of the argument url/error/width/height/mime-type leads to cross site scripting. "

CVE-2023-30093

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-30093

From the Article: "An arbitrary file upload vulnerability in Open Networking Foundation ONOS from version 1.9.0 until 2.7.0 allows attackers to execute arbitrary code via uploading a crafted YAML file."

CVE-2023-25289

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-25289

From the Article: "Directory Traversal vulnerability in virtualreception Digital Receptie version win7sp1_rtm.101119-1850 6.1.7601.1.0.65792 in embedded web server, allows attacker to gain sensitive information via a crafted GET request."

CVE-2023-21491

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-21491

From the Article: "Improper access control vulnerability in ThemeManager prior to SMR May-2023 Release 1 allows local attackers to write arbitrary files with system privilege."

CVE-2023-21493

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

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-21493

From the Article: "Improper access control vulnerability in SemShareFileProvider prior to SMR May-2023 Release 1 allows local attackers to access protected data."

CVE-2023-21494

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-21494

From the Article: "Potential buffer overflow vulnerability in auth api in mm_Authentication.c in Shannon baseband prior to SMR May-2023 Release 1 allows remote attackers to cause invalid memory access."

CVE-2023-21503

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-21503

From the Article: "Potential buffer overflow vulnerability in mm_LteInterRatManagement.c in Shannon baseband prior to SMR May-2023 Release 1 allows remote attackers to cause invalid memory access."

CVE-2023-21504

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-21504

From the Article: "Potential buffer overflow vulnerability in mm_Plmncoordination.c in Shannon baseband prior to SMR May-2023 Release 1 allows remote attackers to cause invalid memory access."

CVE-2023-21486

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-21486

From the Article: "Improper export of android application components vulnerability in ImagePreviewActivity in Call Settings to SMR May-2023 Release 1 allows physical attackers to access some media data stored in sandbox."

Link back to Table of Contents

CVE-2023-30094

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-30094

From the Article: "A stored cross-site scripting (XSS) vulnerability in TotalJS Flow v10 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the platform name field in the settings module."

CVE-2023-30095

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-30095

From the Article: "A stored cross-site scripting (XSS) vulnerability in TotalJS messenger commit b6cf1c9 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the channel description field."

CVE-2023-20126

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-20126

From the Article: "A vulnerability in the web-based management interface of Cisco SPA112 2-Port Phone Adapters could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device."

CVE-2023-2524

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-2524

From the Article: "A vulnerability classified as critical has been found in Control iD RHiD 23.3.19.0. This affects an unknown part of the file /v2/#/. The manipulation leads to direct request. It is possible to initiate the attack remotely."

File Thingie 2.5.7 Shell Upload

Source: https://packetstormsecurity.com/files/172172/filethingie257-shell.txt

Link back to Table of Contents

From the Article: "File Thingie version 2.5.7 remote shell upload exploit. This exploit is based on the vulnerability priorly discovered by Cakes in September of 2019."

UliCMS 2023-1 Sniffing-Vicuna Cross Site Scripting

Source: https://packetstormsecurity.com/files/172174/ulicms20231-xss.txt

From the Article: "UliCMS version 2023-1 Sniffing-Vicuna suffers from a persistent cross site scripting vulnerability."

Jedox 2022.4.2 Database Credential Disclosure

Source: https://packetstormsecurity.com/files/172157/jedox202242-disclose.txt

From the Article: "Jedox version 2022.4.2 has an information disclosure vulnerability in /be/rpc.php that allows remote authenticated users with the appropriate permissions to modify database connections to disclose the clear text credentials via the test connection function."

Jedox 2020.2.5 Groovy-Scripts Remote Code Execution

Source: https://packetstormsecurity.com/files/172155/jedox202025gs-exec.txt

From the Article: "The Jedox Integrator in Jedox version 2020.2.5 allows remote authenticated users to create Jobs to execute arbitrary code via Groovy-scripts."

Jedox 2022.4.2 RPC Interface Remote Code Execution

Source: https://packetstormsecurity.com/files/172151/jedox202242rpc-exec.txt

From the Article: "Jedox version 2022.4.2 has a vulnerability in /be/rpc.php and /be/erpc.php that allows remote authenticated users to load arbitrary PHP classes from the rtn directory and to execute its methods."

Jedox 2020.2.5 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.

Source: https://packetstormsecurity.com/files/172153/jedox202025-xss.txt

From the Article: "Jedox version 2020.2.5 has a persistent cross site scripting vulnerability that allows remote authenticated users to inject arbitrary web scripts or HTML in the logs page via the log module."

PHPJabbers Simple CMS 5.0 Cross Site Scripting

Source: https://packetstormsecurity.com/files/172115/pjsimplecms50-xss.txt

From the Article: "PHPJabbers Simple CMS version 5.0 suffers from a persistent cross site scripting vulnerability."

PHPFusion 9.10.30 Cross Site Scripting

Source: https://packetstormsecurity.com/files/172111/phpfusion91030-xss.txt

From the Article: "PHPFusion version 9.10.30 suffers from a persistent cross site scripting vulnerability."

projectSend r1605 Private File Download

Source: https://packetstormsecurity.com/files/172098/projectsendr1605-disclose.txt

From the Article: "projectSend version r1605 suffers from a private file download vulnerability."

ESET Forwarder 16.0.26.0 Unquoted Service Path

Source: https://packetstormsecurity.com/files/172085/esetforwarder160260-unquotedpath.txt

From the Article: "ESET Forwarder version 16.0.26.0 suffers from an unquoted service path vulnerability."

Link back to Table of Contents

phpMyFAQ 3.1.12 CSV Injection

Source: https://packetstormsecurity.com/files/172097/phpmyfaq3112-inject.txt

From the Article: "phpMyFAQ version 3.1.12 suffers from a CSV injection vulnerability."

Emporium Multi-Vendor 2.1 Cross Site Scripting

Source: https://packetstormsecurity.com/files/172088/emv21-xss.txt

From the Article: "Emporium Multi-Vendor version 2.1 suffers from a cross site scripting vulnerability."

Critical RCE vulnerability in Cisco phone adapters, no update available (CVE-2023-20126)

Source: https://www.helpnetsecurity.com/2023/05/05/cve-2023-20126/

From the Article: "Cisco has revealed the existence of a critical vulnerability (CVE-2023-20126) in the web-based management interface of Cisco SPA112 2-Port Phone Adapters."

CVE-2023-29552: Abusing the SLP Protocol to Launch Massive DDoS Amplification Attacks

Source: https://www.imperva.com/blog/cve-2023-29552-abusing-the-slp-protocol-to-launch-massive-ddos-amplification-attacks/

From the Article: "Service Location Protocol (SLP) is a network protocol designed to simplify the process of discovering and accessing network services. Developed by the Internet Engineering Task Force (IETF) and defined in RFC 2608, SLP eliminates the need for users or administrators to manually configure clients with the addresses of available network services. "

FS-S3900-24T4S Privilege Escalation

Source: https://packetstormsecurity.com/files/172124/fss390024t4s-escalate.txt

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

From the Article: "FS-S3900-24T4S suffers from a privilege escalation vulnerability."

Azure API Management flaws highlight server-side request forgery risks in API development

Source: https://www.csoonline.com/article/3695849/azure-api-management-flaws-highlight-server-side-request-forgery-risks-in-api-development.html

From the Article: "Microsoft recently patched three vulnerabilities in its Azure API Management service, two of which enabled server-side request forgery (SSRF) attacks that could have allowed hackers to access internal Azure assets."

Additional sources:
https://www.csoonline.com/article/3695533/microsoft-patches-3-vulnerabilities-in-azure-api-management.html

Gentoo Linux Security Advisory 202305-06

Source: https://packetstormsecurity.com/files/172107/glsa-202305-06.txt

From the Article: "Gentoo Linux Security Advisory 202305-6 - Multiple vulnerabilities have been discovered in Mozilla Firefox, the worst of which could result in arbitrary code execution. Versions less than 102.7.0:esr are affected."

EasyPHP Webserver 14.1 Path Traversal / Remote Code Execution

Source: https://packetstormsecurity.com/files/172162/easyphpwd141-exectraversal.txt

From the Article: "EasyPHP Webserver version 14.1 suffers from remote code execution and path traversal vulnerabilities."

Jedox 2020.2.5 Configurable Storage Path Remote Code Execution

Source: https://packetstormsecurity.com/files/172154/jedox202025csp-exec.txt

From the Article: "Jedox version 2020.2.5 suffers from a remote code execution vulnerability via the configurable storage path."

Link back to Table of Contents

Debian Security Advisory 5397-1

Source: https://packetstormsecurity.com/files/172133/dsa-5397-1.txt

From the Article: "Debian Linux Security Advisory 5397-1 - Vulnerabilities have been discovered in the WebKitGTK web engine. Luan Herrera discovered that an HTML document may be able to render iframes with sensitive user information. P1umer and Q1IQ discovered that processing maliciously crafted web content may lead to arbitrary code execution. "

Gentoo Linux Security Advisory 202305-23

Source: https://packetstormsecurity.com/files/172132/glsa-202305-23.txt

From the Article: "Gentoo Linux Security Advisory 202305-23 - Multiple vulnerabilities have been discovered in Lua, the worst of which could result in arbitrary code execution."

Codigo Markdown Editor 1.0.1 Code Execution

Source: https://packetstormsecurity.com/files/172180/codigome101-exec.txt

From the Article: "Codigo Markdown Editor version 1.0.1 suffers from an arbitrary code execution vulnerability."

EasyPHP Webserver 14.1 Path Traversal / Remote Code Execution

Source: https://packetstormsecurity.com/files/172162/easyphpwd141-exectraversal.txt

From the Article: "EasyPHP Webserver version 14.1 suffers from remote code execution and path traversal vulnerabilities."

Jedox 2020.2.5 Configurable Storage Path Remote Code Execution

Source: https://packetstormsecurity.com/files/172154/jedox202025csp-exec.txt

Link back to Table of Contents

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

From the Article: "Jedox version 2020.2.5 suffers from a remote code execution vulnerability via the configurable storage path."

Debian Security Advisory 5397-1

Source: https://packetstormsecurity.com/files/172133/dsa-5397-1.txt

From the Article: "Debian Linux Security Advisory 5397-1 - Vulnerabilities have been discovered in the WebKitGTK web engine. Luan Herrera discovered that an HTML document may be able to render iframes with sensitive user information. P1umer and Q1IQ discovered that processing maliciously crafted web content may lead to arbitrary code execution. "

Gentoo Linux Security Advisory 202305-23

Source: https://packetstormsecurity.com/files/172132/glsa-202305-23.txt

From the Article: "Gentoo Linux Security Advisory 202305-23 - Multiple vulnerabilities have been discovered in Lua, the worst of which could result in arbitrary code execution."

CVE-2023-30944

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-30944

From the Article: "The vulnerability was found Moodle which exists due to insufficient sanitization of user-supplied data in external Wiki method for listing pages. A remote attacker can send a specially crafted request to the affected application and execute limited SQL commands within the application database."

Podcasts/Videos

Getting and Staying Cyber Ready with Smarter, Simpler Security and MDR – ESW #316

Source: https://www.scmagazine.com/podcast-segment/getting-and-staying-cyber-ready-with-smarter-simpler-security-and-mdr-esw-316

Link back to Table of Contents
The articles have been 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 Future of Cyber: Lateral Security, Edge Ecosystems, External Attack Surface Mgmt – Christopher Kruegel, Theresa Lanowitz, Vinay Anand – ESW #316

Source: https://www.scmagazine.com/podcast-segment/the-future-of-cyber-lateral-security-edge-ecosystems-external-attack-surface-mgmt-christopher-kruegel-theresa-lanowitz-vinay-anand-esw-316

Sun Tzu Vs Infosec, 2 Weeks of News, AI Trends, & De-Horned Unicorns – ESW #316

Source: https://www.scmagazine.com/podcast-segment/sun-tzu-vs-infosec-2-weeks-of-news-ai-trends-de-horned-unicorns-esw-316

No Pr0nHub 4 U, HTTP Lock Status, Selling Hacking Tools, & Chrome Drops HTTP Lock – PSW #783

Source: https://www.scmagazine.com/podcast-segment/no-pr0nhub-4-u-http-lock-status-selling-hacking-tools-chrome-drops-http-lock-psw-783

Pen Testing Techniques and Jurassic Malware – Rob Fuller – PSW #783

Source: https://www.scmagazine.com/podcast-segment/pen-testing-techniques-and-jurassic-malware-rob-fuller-psw-783

Mitigating AppSec Risk with Systematic Testing and Effective Attack Mitigation – Karl Triebes, Patrick Vandenberg – ASW #239

Source: https://www.scmagazine.com/podcast-segment/mitigating-appsec-risk-with-systematic-testing-and-effective-attack-mitigation-karl-triebes-patrick-vandenberg-asw-239

Application Security Maturity and Frameworks – Francesco Cipollone – ASW #239

Source: https://www.scmagazine.com/podcast-segment/application-security-maturity-

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

and-frameworks-francesco-cipollone-asw-239

Pornhub, LobShot, TMobile, lawsuits, CISA, CERN, AI, Jason Wood, and More – SWN #294

Source: https://www.scmagazine.com/podcast-segment/pornhub-lobshot-tmobile-lawsuits-cisa-cern-ai-jason-wood-and-more-swn-294

Simply Cyber: 🔴 May 5's Top Cyber News NOW! - Ep 360 on Apple Podcasts

Source: https://podcasts.apple.com/us/podcast/may-5s-top-cyber-news-now-ep-360/id1590662228?i=1000611888181

Simply Cyber: 🔴 May 4's Top Cyber News NOW! - Ep 359 on Apple Podcasts

Source: https://podcasts.apple.com/us/podcast/may-4s-top-cyber-news-now-ep-359/id1590662228?i=1000611745366

Simply Cyber: 🔴 May 1's Top Cyber News NOW! - Ep 356 on Apple Podcasts

Source: https://podcasts.apple.com/us/podcast/may-1s-top-cyber-news-now-ep-356/id1590662228?i=1000611349774

Simply Cyber: 🔴 May 2's Top Cyber News NOW! - Ep 357 on Apple Podcasts

Source: https://podcasts.apple.com/us/podcast/may-2s-top-cyber-news-now-ep-357/id1590662228?i=1000611456136

7MS #570: How to Build a Vulnerable Pentest Lab - Part 4

Source: https://7ms.us/7ms-570-how-to-build-a-vulnerable-pentest-lab-part-4/

Link back to Table of Contents
The articles have been 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 Hacker Factory: Unlocking Cybersecurity Success: A Discussion with Sheldon Carmichael | The Hacker Factory Podcast With Phillip Wylie on Apple Podcasts

Source: https://podcasts.apple.com/us/podcast/unlocking-cybersecurity-success-a-discussion/id1581926992?i=1000611899854

OSB OMG and Other News! | TWiT.TV | Age verification, Google Authenticator E2EE, VirusTotal AI, cURL

Source: https://twit.tv/shows/security-now/episodes/921

320: City Jerks, AI animals, and is the BBC hacking again?

Source: https://www.smashingsecurity.com/320-city-jerks-ai-animals-and-is-the-bbc-hacking-again/

Ep 1817 | 5.5.23 DPRK's Kimsuki spearphishes. A standards strategy for AI. Ransomware Task Force retrospective. KillNet's new menu. Ex Uber CSO sentenced for data breach cover-up.

Source: https://thecyberwire.com/podcasts/daily-podcast/1817/notes

Ep 1816 | 5.4.23 Cyberespionage, straight out of Beijing, Teheran, and Moscow. Developments in the criminal underworld. Indictment in a dark web carder case.

Source: https://thecyberwire.com/podcasts/daily-podcast/1816/notes

Ep 1815 | 5.3.23 Iran integrates influence and cyber operations. ChatGPT use and misuse. Trends in the cyber underworld. Hybrid warfare and cyber insurance war clauses.

Source: https://thecyberwire.com/podcasts/daily-podcast/1815/notes

Ep 1814 | 5.2.23 From cryptostealers to CCTV exploits, from Magecart enhancements to coronation phishbait, cybercriminals have been active. (But so have law enforcement agencies.)

Link back to Table of Contents

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

Source: https://thecyberwire.com/podcasts/daily-podcast/1814/notes

Ep 1813 | 5.1.23 FDA warns of biomed device vulnerability. Ransomware's effects continue at US Marshals Service fugitive tracking. US DoJ shifts to disruption of cybercrime. GRU phishing. KillNet's ask-me-anything.

Source: https://thecyberwire.com/podcasts/daily-podcast/1813/notes

Risky Biz News: No jail time for Uber's Joe Sullivan

Source: https://risky.biz/RBNEWS142/

Snake Oilers: Resourcely, Panther and Island

Source: https://risky.biz/snakeoilers17pt2/

Srsly Risky Biz: Iran Fake's It Till It Makes It

Source: https://risky.biz/SRB32/

Risky Biz News: Apple and Google partner to kill AirTag stalking

Source: https://risky.biz/RBNEWS141/

Risky Business #704 -- Why LLMs aren't an exploit bonanza

Source: https://risky.biz/RB704/

Risky Biz News: Hacker exposes Bitcoin addresses operated by Russian intelligence

Source: https://risky.biz/RBNEWS140/

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

Commerce Secretary Raimondo on chips, China and women in the workforce

Source: https://www.marketplace.org/shows/marketplace/commerce-secretary-raimondoon-chips-china-and-women-in-the-workforce/

How Can I Protect My Small Business from Cyber Attacks?

Source: https://sba.thehartford.com/media/podcasts/preventing-cyber-attacks/

From the Article: "Podcast. With a greater percentage of employees working from home, many small business owners are finding themselves more vulnerable to cyber attacks than ever. So what type of precautions do you and your employees need to take in order to protect yourselves from hackers?"

U.S. Has Strategic Clarity on Taiwan, an Interview with Keith Krach

Source: https://www.youtube.com/watch?v=G2z-HRAaQI4

AI will change the way people do their jobs: Keith Krach | Fox News Video

Source: https://www.foxnews.com/video/6326940360112

Semiconductor slump worse than feared, but recovery in sight

Source: https://www.theregister.com/2023/04/26/semiconductor_slump_worse_than_feared/

From the Article: "Next year's revenue forecast to surpass the halcyon days of 2022"

In Focus: Impact of Artificial Intelligence (AI) on Supply Chain

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

What's next for experimental AI projects in the C4ISR sphere

Link back to Table of Contents
The articles have been 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.militarytimes.com/video/2023/05/01/whats-next-for-experimental-ai-projects-in-the-c4isr-sphere/

Investing in electronic warfare

Source: https://www.militarytimes.com/video/2023/05/01/investing-in-electronic-warfare/

What's next for experimental AI projects in the C4ISR sphere

Source: https://www.militarytimes.com/video/2023/05/01/whats-next-for-experimental-ai-projects-in-the-c4isr-sphere/

Investing in electronic warfare

Source: https://www.militarytimes.com/video/2023/05/01/investing-in-electronic-warfare/

Dallas ransomware attack: Here's the latest information we know - YouTube

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

From the Article: "We have passed the 48 hour mark since the City of Dallas was attacked by hackers."

Live Masterclass | A Master Class on IT Security: Roger Grimes Teaches Ransomware Mitigation

Source: https://www.bankinfosecurity.com/webinars/live-webinar-protect-govern-sensitive-data-w-4667

From the Article: "Cyber-criminals have become thoughtful about ransomware attacks; taking time to maximize your organization’s potential damage and their payoff. Protecting your network from this growing threat is more important than ever. And nobody knows this more than Roger Grimes, Data-Driven Defense Evangelist at KnowBe4."

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

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.”

Department of Defense Catalog Data Standard
Source: https://www.acq.osd.mil/dpap/dars/opencases/dfarscasenum/dfars.pdf

From the Article: “Case Number 2023-D019. Implements a requirement to use the Department of Defense Catalog Data Standard when contracting for certain commercial items and services, and other potential use cases to standardize the collection of data for supplies and services obtained from contractor catalogs. Status: DARC Director tasked Acquisition Technology & Information (DFARS) to draft proposed DFARS rule. Report due 06/14/2023.”

Open Market Micro-purchase Representation
Source: https://www.acq.osd.mil/dpap/dars/opencases/dfarscasenum/dfars.pdf

From the Article: “Case Number 2023-D018. Implements a representation requirement for open market micro-purchases in connection with the prohibition on contracting for certain telecommunications and video surveillance services or equipment at FAR subpart 13.201(j). Status: DARC Director tasked Acquisition Technology and Information Team to draft proposed DFARS rule. Report due 06/14/2023.”

Prohibition on Certain Semiconductor Products and Services
Source: https://www.acq.osd.mil/dpap/dars/opencases/farcasenum/far.pdf

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

From the Article: “Case Number 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 date extended to 05/17/2023.”

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: DARS Regulatory Control Officer submitted draft interim DFARS rule to OIRA. OIRA reviewing."

Strategic and Critical Materials Stockpiling Act Reform
Source: https://www.acq.osd.mil/dpap/dars/opencases/dfarscasenum/dfars.pdf

From the Article: "Case Number 2023-D014, Part Number 225: Strategic and Critical Materials Stockpiling Act Reform. Implements section 1411 of the NDAA for FY 2023 (Pub. L. 117-263); which repeals 10 U.S.C. 187 the Strategic Materials Protection Board, and amends 50 U.S.C. 98h-1 section 10, Strategic and Critical Materials Board of Directors. Status: DARC Director tasked Acquisition Law International Acquisition team to draft proposed DFARS rule. Report due 05/17/2023."

Modification of Cooperative Research and Development Project Authority
Source: https://www.acq.osd.mil/dpap/dars/opencases/dfarscasenum/dfars.pdf

From the Article: "Case Number 2023-D013, Part Number 225.8: Modification of Cooperative Research and Development Project Authority. Implements section 211 of the NDAA for FY 2023 (Pub. L. 117-263) which amends 10 U.S.C. 2350a(a) (2) to expand the scope of 225.871, North Atlantic Treaty Organization (NATO) cooperative projects to also include Cooperative Research and Development Projects to include other allied and friendly foreign countries under the European Union and the European Defense Agency, the European Commission, and the Council of the European Union and their suborganizations. Status: DARC Director tasked Acquisition Law International Acquisition team to draft proposed DFARS rule. Report due 05/24/2023."

Prohibition on Procurement of ForeignMade Unmanned Aircraft Systems
Source: https://www.acq.osd.mil/dpap/dars/opencases/dfarscasenum/dfars.pdf

From the Article: "Case Number 2023-D012, Part Number 204, 252: Prohibition on Procurement of ForeignMade Unmanned Aircraft Systems. Implements section 848 of the NDAA for FY 2020 (Pub L. 116-92), as amended by section 817 of the FY 2023 NDAA (Pub. L. 117-263), which prohibits the procurement of certain foreign-made unmanned aircraft systems by the Department of Defense. Status: DARC Director tasked Acquisition Technology & Information Team to draft proposed DFARS rule. Report due date extended to 06/07/2023."

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.

Establishing FAR Part 40
Source: https://www.acq.osd.mil/dpap/dars/opencases/farcasenum/far.pdf

From the Article: "Case Number 2022-010, Part Number 40: Establishing FAR Part 40. The purpose of this case is to amend the FAR to create a new FAR part, part 40, which will be the new location for cybersecurity supply chain requirements in the FAR. Status: DARC Director tasked staff to draft final FAR rule. Report due date extended to 06/14/2023"

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: CAAC Chair sent draft proposed FAR rule to OIRA. OIRA reviewing."

(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.

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

DAR and FAR staff resolving draft proposed FAR rule open issues."

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

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

Assessing Contractor Implementation of Cybersecurity Requirements
Source: https://www.acq.osd.mil/dpap/dars/opencases/dfarscasenum/dfars.pdf

From the Article: "Case Number 2019-D041, Part Number 204.73, 204.75, 212.301, 217.207, 252.204-7019, 252.204-7020, 252.204-7021: Assessing Contractor Implementation of Cybersecurity Requirements. Implements a DoD certification process, known as the Cybersecurity Maturity Model Certification (CMMC), that measures a company's maturity and institutionalization of cybersecurity practices and processes. Partially implements section 1648 of the FY20 NDAA. (See DFARS case 2022-D017 for the NIST SP 800-171 DoD assessment requirements.) Status: DARC Director tasked Adhoc Team to review public comments, draft final DFARS rule. Report due date extended to 06/14/2023."

(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: DARS Regulatory Control Officer submitted draft proposed DFARS rule to OIRA. OIRA reviewing."

NIST SP 800-171 DoD Assessment Requirements

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

Source: https://www.acq.osd.mil/dpap/dars/opencases/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 06/21/2023."

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 06/07/2023."

Enhanced Price Preferences for Critical Components and Critical Items
Source: https://www.acq.osd.mil/dpap/dars/opencases/farcasenum/far.pdf

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

extended to 06/07/2023."

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

Critical Infrastructure Organizations Urged to Identify Risky Communications Equipment

Source: https://www.securityweek.com/critical-infrastructure-organizations-urged-to-identify-risky-communications-equipment/

Summary: Updated guidance from CISA 1-May-2023 reminds critical infrastructure operators to review communications equipment and verify it is not on the FCC covered list of risky equipment.

Link to FCC list: https://www.fcc.gov/supplychain/coveredlist

Reports - Industry

Resilinc's Special Report: Wuxi Fire Disrupts Semiconductor Supply Chains

Source: https://www.resilinc.com/learning-center/white-papers-reports/resilinc-special-report-wuxi-fire-disrupts-semiconductor-supply-chains/

Debt limit drama pdf

Source: https://www.moodysanalytics.com/-/media/article/2023/debt-limit-drama.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.

China's Grand Strategy for Global Data Dominance

Source: https://www.scribd.com/document/638301750/China-s-Grand-Strategy-for-Global-Data-Dominance

Semiconductor Sector Valuation Update 2022 - TD Cowen Continental Europe

Source: https://www.cowen.eu/en/insights/semiconductor-update-2022/

The 2023 SIA Factbook: Your Source for Semiconductor Industry Data

Source: https://www.semiconductors.org/the-2023-sia-factbook-your-source-for-semiconductor-industry-data/

Geopolitics may bring dramatic shifts in semiconductor industry

Source: https://www.digitimes.com/reportdownload/index.asp?openid=4

Resilinc Annual Report 2022 - Turbulence

Source: https://www.resilinc.com/learning-center/white-papers-reports/resilinc-annual-report-2022-turbulence/

Legislation

Senate Committee reintroduces bipartisan bill to protect commercial satellites from cybersecurity threats

Source: https://industrialcyber.co/regulation-standards-and-compliance/senate-committee-reintroduces-bipartisan-bill-to-protect-commercial-satellites-from-cybersecurity-threats/

From the Article: "Members of the U.S. Senate Committee on Homeland Security & Governmental Affairs reintroduced bipartisan legislation that would require the Cybersecurity and Infrastructure Security Agency (CISA) to help protect commercial satellite owners and operators from disruptive cyber-attacks. "

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

Senators unveil Taiwan tax plan to spur semiconductor investment

Source: https://www.digitimes.com/news/a20230505VL209/us-taiwan-trade-semiconductor-investment.html

From the Article: "A bipartisan group of US senators introduced legislation that would allow President Joe Biden to sign a tax agreement with Taiwan, addressing an issue that businesses on both sides have pointed to as a barrier for further investment."

White House

FACT SHEET: President Biden Delivers Update on His Strategy to Build on America's Small Business Boom, while Speaker McCarthy and House Republicans Threaten to Harm Small Businesses and Eliminate Jobs | The White House

Source: https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/01/fact-sheet-president-biden-delivers-update-on-his-strategy-to-build-on-americas-small-business-boom-while-speak-mccarthy-and-house-republicans-threaten-to-harm-small-businesses-and-eliminat/

FACT SHEET: Biden-Harris Administration Announces National Standards Strategy for Critical and Emerging Technology | The White House

Source: https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/04/fact-sheet-biden-harris-administration-announces-national-standards-strategy-for-critical-and-emerging-technology/

Remarks by President Biden in Meeting with His Investing in America Cabinet | The White House

Source: https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/05/remarks-by-president-biden-in-meeting-with-his-investing-in-america-cabinet/

Link back to Table of Contents

Readout of White House Convening on Advancing Clean Buildings | The White House

Source: https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/05/readout-of-white-house-convening-on-advancing-clean-buildings/

Remarks by Vice President Harris on Investing in Small Business Manufacturing | The White House

Source: https://www.whitehouse.gov/briefing-room/speeches-remarks/2023/05/05/remarks-by-vice-president-harris-on-investing-in-small-business-manufacturing/

Readout of White House Meeting with CEOs on Advancing Responsible Artificial Intelligence Innovation | The White House

Source: https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/04/readout-of-white-house-meeting-with-ceos-on-advancing-responsible-artificial-intelligence-innovation/

Statement from Vice President Harris After Meeting with CEOs on Advancing Responsible Artificial Intelligence Innovation | The White House

Source: https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/04/statement-from-vice-president-harris-after-meeting-with-ceos-on-advancing-responsible-artificial-intelligence-innovation/

FACT SHEET: Vice President Harris Celebrates Small Business and Manufacturing Boom | The White House

Source: https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/04/fact-sheet-vice-president-harris-celebrates-small-business-and-manufacturing-boom/

Background Press Call on New Artificial Intelligence Announcements | The White House

Source: https://www.whitehouse.gov/briefing-room/press-

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

briefings/2023/05/04/background-press-call-on-new-artificial-intelligence-announcements/

FACT SHEET: Biden-Harris Administration Announces National Standards Strategy for Critical and Emerging Technology | The White House

Source: https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/04/fact-sheet-biden-harris-administration-announces-national-standards-strategy-for-critical-and-emerging-technology/

FACT SHEET: Biden-Harris Administration Announces New Actions to Promote Responsible AI Innovation that Protects Americans' Rights and Safety | The White House

Source: https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/04/fact-sheet-biden-harris-administration-announces-new-actions-to-promote-responsible-ai-innovation-that-protects-americans-rights-and-safety/

STATE FACT SHEETS: MAGA House Republicans' Default on America Act Would Have Devastating Impacts Across America | The White House

Source: https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/02/state-fact-sheets-maga-house-republicans-default-on-america-act-would-have-devastating-impacts-across-america/

Articles of Interest

IT Services in City of Dallas Impacted by Royal Ransomware Attack

Source: https://cyberintelmag.com/attacks-data-breaches/it-services-in-city-of-dallas-impacted-by-royal-ransomware-attack/

From the Article: "Due to a Royal ransomware attack, the City of Dallas in Texas had to take down some of its IT systems to stop the attack's spread. According to US census figures, Dallas has a population of nearly 2.6 million, making it the ninth-largest city in the country."

Additional sources:
https://securityaffairs.com/145723/cyber-crime/city-of-dallas-ransomware-attack.html
Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

https://siliconangle.com/2023/05/04/dallas-emergency-services-systems-knocked-offline-royal-ransomware-attack/

https://communityimpact.com/dallas-fort-worth/lake-highlands-lakewood/government/2023/05/04/ransomware-attack-impacts-dallas-services-city-network/

https://news.yahoo.com/dallas-animal-services-crippled-city-223753470.html

https://www.wbap.com/2023/05/06/listen-dallas-mayor-talks-second-term-ransomware/

https://www.dallasnews.com/news/public-safety/2023/05/07/dallas-fire-rescue-police-see-delays-and-mistakes-answering-calls-after-ransomware-attack/

https://www.infosecurity-magazine.com/news/dallas-police-compromised/

https://informationsecuritybuzz.com/dallas-city-hit-by-ransomware-assault-affects-2-6-million-people/

https://www.helpnetsecurity.com/2023/05/04/dallas-ransomware/

https://heimdalsecurity.com/blog/royal-ransomware-targets-the-city-of-dallas-in-ransomware-attack/

https://www.bankinfosecurity.com/breach-roundup-royal-ransomware-does-dallas-a-21976

https://www.darkreading.com/attacks-breaches/dallas-city-systems-taken-down-by-royal-ransomware

https://www.infosecurity-magazine.com/news/dallas-police-compromised/

https://www.nbcdfw.com/news/local/city-of-dallas-continues-battling-ransomware-attack-for-third-day/3251877/

https://cisoseries.com/cyber-security-headlines-royal-ransoms-dallas-new-papercut-exploit-cisas-mirai-warning/

https://www.fox4news.com/news/dallas-animal-services-crippled-by-city-ransomware-attack

https://www.dallasnews.com/news/2023/05/05/as-dallas-ransomware-attack-stretches-

Link back to Table of Contents

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

into-day-3-other-texas-cities-boost-cybersecurity/

https://wtvbam.com/2023/05/05/fbi-says-it-is-coordinating-with-city-of-dallas-over-ransomware-incident/

https://securityboulevard.com/2023/05/dallas-royal-ransomware-richixbw/

https://www.dallasnews.com/news/2023/05/04/what-to-know-about-ransomware-and-royal-the-group-behind-the-cyber-attack-on-dallas/

https://www.dmagazine.com/frontburner/2023/05/three-days-in-to-a-ransomware-attack-dallas-city-hall-is-giving-few-details/

https://ktvz.com/news/2023/05/05/critical-city-services-in-dallas-still-dealing-with-ransomware-attack/

https://www.securitysystemsnews.com/article/city-of-dallas-struck-by-royal-ransomware

https://www.theregister.com/2023/05/05/dallas_royal_ransomeare/

https://www.dallasobserver.com/news/hacked-dallas-ransomware-attack-disrupts-city-services-16516621

https://www.securitymagazine.com/articles/99310-city-of-dallas-recovers-after-recent-ransomware-attack

https://www.insurancejournal.com/news/southcentral/2023/05/05/719684.htm

https://www.cybersecuritydive.com/news/dallas-ransomware-recovery/649555/

https://www.scmagazine.com/brief/ransomware/dallas-impacted-by-royal-ransomware-attack

https://www.ntd.com/city-of-dallas-hit-by-ransomware-attack-multiple-city-services-impeded_917286.html

https://www.cybersecurityconnect.com.au/critical-infrastructure/9013-city-of-dallas-systems-taken-offline-by-ransomware-attack

https://www.policemag.com/home/featured/news/15447062/dallas-police-significantly-impacted-by-ransomware-attack

https://easttexasradio.com/city-of-dallas-hit-by-ransomware/

Link back to Table of Contents

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

https://dallas.culturemap.com/news/city-life/ransomware-dallas-city-hall-servers/

https://www.audacy.com/krld/news/national/city-of-dallas-investigates-ransomware-attack-that-affected-multiple-services

https://www.wfaa.com/video/news/local/who-is-behind-the-ransomware-attack-against-the-city-of-dallas/287-44e55e73-ddc3-48e7-8baf-f39fe033cb5c

https://www.reuters.com/world/us/dallas-disrupted-by-hackers-courts-closed-police-fire-sites-offline-2023-05-04/

https://www.cbsnews.com/texas/video/critical-city-services-in-dallas-still-dealing-with-ransomware-attack/

https://www.fox4news.com/news/city-of-dallas-services-still-affected-by-ransomware-attack

T-Mobile Hacked – Attackers Accessed Over 37M Sensitive Data

Source: https://gbhackers.com/t-mobile-hacked-data/

From the Article: "T-Mobile recently confirmed another hack, the second this year and ninth since 2018, revealing customer data and account PINs. While T-Mobile confirmed a recent system detection that revealed a threat actor had accessed a small number of accounts, which compromised limited information."

Additional sources:
https://informationsecuritybuzz.com/t-mobile-data-breach-the-second/

https://news.hitb.org/content/t-mobile-discloses-2nd-data-breach-2023-one-leaking-account-pins-and-more

https://www.darkreading.com/attacks-breaches/t-mobile-experiences-another-data-breach

https://www.blackhatethicalhacking.com/news/t-mobile-discloses-second-data-breach-of-2023-affecting-hundreds-of-customers/

https://www.scmagazine.com/news/breach/t-mobile-security-breach

https://www.helpnetsecurity.com/2023/05/03/t-mobile-breach-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.

https://www.infosecurity-magazine.com/news/tmobile-reveals-second-breach-of/

$1.1M paid to resolve ransomware attack on California county - Greenwich Time

Source: https://www.greenwichtime.com/business/article/1-1m-paid-to-resolve-ransomware-attack-on-18082108.php

From the Article: "The San Bernardino County Sheriff's Department announced in April that a “network disruption” was being investigated by information technology staff and forensic specialists, and that the FBI and Department of Homeland Security were notified."

Additional sources:
https://www.ivpressonline.com/business/1-1m-paid-to-resolve-ransomware-attack-on-california-county/article_4ffb9718-b90e-590e-b04b-aa533b0fed70.html

https://www.vvdailypress.com/story/news/crime/2023/05/05/county-pays-hacker-1-1-million-ransom-after-cyber-attack/70190226007/

https://www.msn.com/en-us/news/us/san-bernardino-county-pays-dollar11-million-to-settle-ransomware-attack/ar-AA1aNVjP

https://thebrunswicknews.com/news/business/san-bernardino-county-pays-1-1-million-ransom-over-sheriff-s-department-hack/article_373ec79d-80a9-5bf0-ab0b-74771ce9cc28.html

https://securityaffairs.com/145892/cyber-crime/san-bernardino-county-sheriff-paid-ransom.html

https://www.theepochtimes.com/california-sheriffs-department-pays-1-1-million-in-ransom-to-hackers-after-cyberattack_5247513.html

Rochester Public Schools confirms ransomware attack; says it did not pay a ransom

Source: https://www.postbulletin.com/news/local/rochester-public-schools-confirms-ransomeware-attack-says-it-did-not-pay-a-ransom

From the Article: "The School District released an update on the ongoing situation Thursday, May 4, just shy of a month since unusual activity was first noticed on its

network."

Additional sources:
https://www.govtech.com/education/k-12/rochester-schools-confirm-ransomware-attack-didnt-pay

https://bringmethenews.com/minnesota-news/ransomware-attack-confirmed-at-rochester-public-schools-fbi-alerted

https://www.startribune.com/rochester-schools-confirm-district-suffered-ransomware-attack/600272527/

https://www.kimt.com/news/rochester-school-district-says-it-was-victim-of-a-ransomware-attack/article_5d5d385e-eab6-11ed-af43-ab171825bd76.html

https://www.kttc.com/2023/05/05/cybersecurity-experts-comment-rps-ransomware-attack/

The Ransomware Gang Targets University Alert Systems

Source: https://www.cysecurity.news/2023/05/the-ransomware-gang-targets-university.html

From the Article: ""RamAlert," an emergency broadcast system used by Bluefield University to communicate with its students and staff, has been hijacked by the Avos ransomware gang. The gang sent SMS texts and emails informing them that their data had been stolen and was in the process of being released."

Additional sources:
https://www.cybertalk.org/2023/05/05/ransomware-gang-hijacks-colleges-emergency-alert-system-threatens-students/

https://www.bleepingcomputer.com/news/security/ransomware-gang-hijacks-university-alert-system-to-issue-threats/

https://www.infosecurity-magazine.com/news/ransomware-actors-extort/

https://www.techradar.com/news/ransomware-gang-uses-emergency-broadcasts-to-tell-university-theyve-been-attacked

https://www.infosecurity-magazine.com/news/ransomware-actors-extort/

Link back to Table of Contents

The articles have been 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 'Lobshot' hVNC Malware Used by Russian Cybercriminals

Source: https://www.securityweek.com/new-lobshot-hvnc-malware-used-by-russian-cybercriminals/

From the Article: "Russian cybercrime group TA505 has been observed using new hVNC malware called Lobshot in recent attacks."

Additional sources:
https://www.blackhatethicalhacking.com/news/new-malware-lobshot-secretly-takes-over-windows-devices-via-google-ads/

https://cyberintelmag.com/malware-viruses/new-lobshot-malware-may-allow-hackers-access-to-windows-devices-via-covert-vnc/

https://securityaffairs.com/145597/malware/lobshot-malware-hvnc.html

https://www.cysecurity.news/2023/05/google-ads-exploited-to-tempt-corporate.html

FBI and Ukrainian police seized 9 crypto exchanges used by cybercriminals

Source: https://securityaffairs.com/145668/cyber-crime/crypto-exchanges-seizure.html

From the Article: "The Cyber Police Department together with the Main Investigative Department of the National Police, the Office of the Prosecutor General of Ukraine and in cooperation with the FBI conducted an international operation that seized nine crypto exchanges used by cybercriminal groups to launder profits from illegal activities, including ransomware attacks and online fraud."

Additional sources:
https://www.bankinfosecurity.com/cryptohack-roundup-crypto-exchange-seizures-a-21980

https://www.cysecurity.news/2023/05/cryptocurrency-exchanges-linked-to.html

https://www.bleepingcomputer.com/news/security/fbi-seizes-9-crypto-exchanges-used-to-launder-ransomware-payments/

https://informationsecuritybuzz.com/fbi-uncovers-9-crypto-exchanges-ransomware-

laundering/

Former Uber CSO avoids prison for concealing data breach

Source: https://www.helpnetsecurity.com/2023/05/05/joe-sullivan-sentenced/

From the Article: "Joe Sullivan, the former Uber CSO who has been convicted last year for attempting to cover up a data breach Uber suffered in 2016 and kept it hidden from the Federal Trade Commission (FTC), has been sentenced to three years of probation plus 200 hours of community service. "

Additional sources:
https://gizmodo.com/uber-security-joe-sullivan-sentenced-prison-data-breach-1850403347

https://www.darkreading.com/attacks-breaches/judge-spares-former-uber-ciso-jail-time-over-2016-data-breach-charges

https://www.cybersecuritydive.com/news/uber-cso-prison-ransomware/649561/

Leaked Files Show Extent of Ransomware Group's Access to Western Digital Systems

Source: https://www.securityweek.com/leaked-files-show-extent-of-ransomware-groups-access-to-western-digital-systems/

From the Article: "A ransomware group has leaked files showing the extent of their access to Western Digital systems and it appears that the hackers were closely monitoring the company's initial response to the breach from within its network."

Additional sources:
https://www.darkreading.com/remote-workforce/ransomware-group-trolls-western-digital-threat-hunters-

https://www.bleepingcomputer.com/news/security/hackers-leak-images-to-taunt-western-digitals-cyberattack-response/

https://www.cysecurity.news/2023/05/hackers-leak-photos-to-mock-western.html

Link back to Table of Contents

New Decoy Dog Malware Toolkit Uncovered: Targeting Enterprise Networks

Source: https://thehackernews.com/2023/05/new-decoy-dog-malware-toolkit-uncovered.html

From the Article: "An analysis of over 70 billion DNS records has led to the discovery of a new sophisticated malware toolkit dubbed Decoy Dog targeting enterprise networks."

Additional sources:
https://securityaffairs.com/145580/malware/decoy-dog-sophisticated-malware-toolkit.html

https://heimdalsecurity.com/blog/new-decoy-dog-malware-toolkit-targets-enterprise-networks/

https://www.cysecurity.news/2023/05/uncovering-decoy-dog-c2-exploit.html

Court Rejects Merck Insurers' Attempt to Refuse Coverage for NotPetya Damages

Source: https://www.darkreading.com/attacks-breaches/court-rejects-merck-insurers-attempts-to-refuse-coverage-for-notpetya-damages

From the Article: "Insurers unsuccessfully argued Merck's $1.4B in losses following NotPetya cyberattack fell under wartime exclusion."

Additional sources:
https://www.csoonline.com/article/3695573/the-merck-appeal-cyber-insurance-and-the-definition-of-war.html

https://www.securingindustry.com/pharmaceuticals/court-says-insurers-must-pay-merck-over-cyberattack/s40/a15271/

Ransomware Gangs Are Shifting Their Attacks to Smaller Companies - Jackson Progress-Argus

Source: https://www.jacksonprogress-argus.com/arena/thestreet/ransomware-gangs-are-shifting-their-attacks-to-smaller-companies/article_15e1224a-7357-5056-adec-5b5b5a02d397.html

From the Article: "Attacks have surged in past 12 months as hackers go after companies in the manufacturing, professional, scientific and technical services

Link back to Table of Contents

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

industries."

Additional sources:
https://www.albanyherald.com/arena/thestreet/ransomware-gangs-are-shifting-their-attacks-to-smaller-companies/article_abcb7629-6291-5603-96ea-94d1757dfb08.html

Tennessee Health System Stops All Operations Amid Cyberattack Recovery

Source: https://www.scmagazine.com/news/breach/tennessee-health-system-stops-all-operations-amid-cyberattack-recovery

From the Article: "Murfreesboro Medical Clinic & SurgiCenter was forced offline after a cyberattack was deployed on April 22. In response, the Tennessee provider closed all operations and launched an emergency shutdown of the network to prevent the attack from spreading."

Additional sources:
https://www.bankinfosecurity.com/mmc-attack-a-21996

Cybersecurity for Level 0,1 devices is underdeveloped

Source: https://www.controlglobal.com/blogs/unfettered/blog/33004947/cybersecurity-for-level-01-devices-is-underdeveloped

From the article: “My paper, “Challenges in Federal Facility Control System Cyber Security, Including Level 0 and 1 Devices” was published on the National Academies of Sciences web site. The paper addresses the problem that cybersecurity for Level 0,1 devices - which include sensors and the Industrial Internet of Things - is underdeveloped. The Federal Facilities Council white paper addresses changes to improve cybersecurity, productivity, process safety, predictive maintenance, and resilience, while also breaking down cultural and organizational barriers. This applies to all buildings including office buildings, data centers, laboratories, manufacturing facilities, and others. The continuing gap in understanding the importance of cyber secure process instrumentation can be seen from the March 2023 CISA RIPDWG White Paper, “Research, Development, and Innovation for Enhancing Resilience of Cyber-Physical Critical Infrastructure Needs and Strategic Action” which did not mention the need for cyber secure process instrumentation.”

Link back to Table of Contents

Dulles CBP Officers Seize Nearly $290K in Counterfeit Apple AirPods and Apple Watches

Source: https://www.cbp.gov/newsroom/local-media-release/dulles-cbp-officers-seize-nearly-290k-counterfeit-apple-airpods-and

From the article: “Apple products are popular, and so that explains why U.S. Customs and Border Protection officers would encounter nearly $290,000 in AirPods and Apple Watch knockoffs recently shipped from China in air cargo imports to Washington Dulles International Airport.”

Hackers are Breaking Into AT&T to Steal Cryptocurrency

Source: https://www.cysecurity.news/2023/05/hackers-are-breaking-into-at-to-steal.html

From the Article: "In recent news, individuals with AT&T email addresses are being targeted by unknown hackers who are using their access to break into victims' cryptocurrency exchange accounts and steal their digital assets. Cryptocurrency exchanges are online platforms that allow users to buy, sell, and trade digital currencies like Bitcoin and Ethereum. "

Additional sources:
https://research.checkpoint.com/2023/1st-may-threat-intelligence-report/

Critical Vulnerabilities Found In Illumina Universal Copy Service Devices

Source: https://latesthackingnews.com/2023/05/01/critical-vulnerabilities-found-in-illumina-universal-copy-service-devices/

From the Article: "Illumina is a US-based biotechnology firm that develops and markets equipment for genetic analysis and related biological and medical functions. The firm develops key devices for gene sequencing, gene expression, genotyping, and proteomics. The Universal Copy Service is a key software for DNA sequencing in health and research facilities."

Additional sources:
https://www.darkreading.com/ics-ot/medical-device-flaws-gets-new-twist-with-dna-sequencer-vulnerabilities

Russian hackers use fake Windows updates to target Ukrainian government

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

Source: https://www.blackhatethicalhacking.com/news/russian-hackers-use-fake-windows-updates-to-target-ukrainian-government/

From the Article: "Russian state-sponsored hacking group APT28 (also known as Fancy Bear) is targeting various government bodies in Ukraine with malicious emails, posing as instructions on how to upgrade Windows for cyberattack defense, according to the Computer Emergency Response Team of Ukraine (CERT-UA)."

Netflix MH370: The plane that wasn't hacked

Source: https://www.pentestpartners.com/security-blog/netflix-mh370-the-plane-that-wasnt-hacked/

Summary: PenTest partners goes through an analysis of a recent documentary of MH370...and a very good introduction to aircraft networking.

Critical Siemens RTU Vulnerability Could Allow Hackers to Destabilize Power Grid

Source: https://www.securityweek.com/critical-siemens-rtu-vulnerability-could-allow-hackers-to-destabilize-power-grid/

Summary: "Greil pointed out that Siemens Sicam products are among the first devices in the world to receive 'maturity level 4' certification in the Industrial Cyber Security category. This certification, IEC62443-4-1, indicates that security was an important factor throughout the design and development process and that the product has undergone rigorous testing. "

An NCIS Agent's Fight Against Counterfeit and Critical Fraudulent Parts In The Military

Source: https://theaviationist.com/2023/05/06/an-ncis-agents-fight-against-counterfeit-and-critical-fraudulent-parts/

Summary: Interview with an NCIS agent and how NCIS and NAVAIR battled counterfeit and critical fraudulent part in the military.

The hidden security risks in tech layoffs and how to mitigate them

Source: https://www.csoonline.com/article/3695070/the-hidden-security-risks-in-tech-layoffs-

Link back to Table of Contents

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

and-how-to-mitigate-them.html

From the Article: "In the shadowy corners of the tech world, there are plenty of stories of admins locking organizations out of their own IT environment, greedy employees selling data, or security engineers backdooring the network. "

ViperSoftX uses more sophisticated encryption and anti-analysis techniques

Source: https://securityaffairs.com/145464/malware/vipersoftx-sophisticated-encryption.html

From the Article: "Trend Micro researchers observed a new ViperSoftX malware campaign that unlike previous attacks relies on DLL sideloading for its arrival and execution technique."

Targeted: Hackers Exploit Vulnerable Veeam Backup Servers with FIN7 Tactics

Source: https://www.cysecurity.news/2023/05/targeted-hackers-exploit-vulnerable.html

From the Article: "Veeam Backup and Replication software is a popular choice for many organizations to protect their critical data. However, recent reports have revealed that hackers are targeting vulnerable Veeam backup servers that are exposed online, leaving organizations at risk of data theft and other cyberattacks. "

The Persistent Threat of Ransomware: RSA Conference 2023 Highlights

Source: https://www.cysecurity.news/2023/05/the-persistent-threat-of-ransomware-rsa.html

From the Article: "The cybersecurity industry's highest-profile annual gathering, the RSA Conference, has focused heavily on the ongoing and increasing threat of ransomware. Last year, 68% of all cyberattacks involved ransomware, according to cybersecurity firm Sophos. "

Amnesty International Takes a While to Disclose the Data Breach From December

Source: https://www.cysecurity.news/2023/05/amnesty-international-takes-while-to.html

From the Article: "Amnesty International Australia notified supporters via email last Friday that their data might be at risk owing to "anomalous activity" discovered in its IT 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.

This New macOS Info-stealer in Town is Targeting Crypto Wallets

Source: https://www.cysecurity.news/2023/05/this-new-macos-info-stealer-in-town-is.html

From the Article: "A new info-stealer malware has been identified, designed to steal a wide range of personal data, comprising local files, cookies, financial information, and passwords stored in macOS browsers."

How AI is Helping Threat Actors to Launch Cyber Attacks

Source: https://www.cysecurity.news/2023/04/how-ai-is-helping-threat-actors-to.html

From the Article: "Artificial intelligence offers great promise, and while many tech enthusiasts are enthusiastic about it, hackers are also looking to this technology to aid their illicit activities. The field of artificial intelligence is interesting, but it may also make us nervous. Therefore, how might AI support online criminals? "

Ransomware Clop and LockBit Attacked PaperCut Servers

Source: https://www.cysecurity.news/2023/04/ransomware-clop-and-lockbit-attacked.html

From the Article: "A Microsoft spokesperson stated in a statement that recent attacks that exploited two vulnerabilities in the PaperCut print management software are likely associated with an affiliate program for the Clop ransomware. "

DOJ Prioritizes Disruptions Over Arrests in Cyberattack Cases

Source: https://www.cysecurity.news/2023/04/doj-prioritizes-disruptions-over.html

From the Article: "The Department of Justice is requesting its prosecutors and investigators to focus less on prosecutions and more on disruption and protection when it comes to cyberattacks, according to US Deputy Attorney General Lisa Monaco, who spoke to attendees at the RSA Conference. "

Chinese APT Group Hijacks Software Updates for Malware Delivery

Source: https://www.cysecurity.news/2023/04/chinese-apt-group-hijacks-software.html

From the Article: "An advanced persistent threat (APT) group from China, known as Evasive

Link back to Table of Contents

Panda, has been discovered to be hijacking legitimate software update channels of Chinese-developed applications to deliver custom malware to individuals in China and Nigeria for cyber-espionage purposes."

What the Cybersecurity Industry Can Learn From the SVB Crisis

Source: https://www.darkreading.com/risk/what-the-cybersecurity-industry-can-learn-from-the-svb-crisis

From the Article: "The banking industry has safeguards designed to mitigate financial risk, something the cybersecurity industry can learn from."

Cisco Offers Customers New Ways To Tame Today's Threat Landscape

Source: https://www.darkreading.com/threat-intelligence/cisco-offers-customers-new-ways-to-tame-today-s-threat-landscape

From the Article: "Cisco's Tom Gillis joins Dark Reading's Terry Sweeney at Dark Reading News Desk during RSA Conference to discuss the current threat landscape."

Aigital Wireless-N Repeater Mini_Router.0.131229 Remote Command Execution

Source: https://packetstormsecurity.com/files/172061/aigitalwireless-exec.txt

From the Article: "Aigital Wireless-N Repeater version Mini_Router.0.131229 suffers from a remote command execution vulnerability."

Israel's Prime Minister has his Facebook account hijacked, website knocked offline

Source: https://www.bitdefender.com/blog/hotforsecurity/israels-prime-minister-has-his-facebook-account-hijacked-website-knocked-offline/

From the Article: "Wednesday was the official Independence Day of Israel, and the event was "celebrated" in typical style by malicious hackers."

Cybercriminals use proxies to legitimize fraudulent requests

Link back to Table of Contents
The articles have been 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/2023/05/01/malicious-bot-attacks/

From the Article: "Bot attacks were previously seen as relatively inconsequential type of online fraud, and that mentality has persisted even as threat actors have gained the ability to cause significant damage to revenue and brand reputation, according to HUMAN."

Using just-in-time access to reduce cloud security risk

Source: https://www.helpnetsecurity.com/2023/05/01/using-jit-privileged-access/

From the Article: "Excessive privileges are a continuing headache for security professionals. As more organizations migrate assets to the cloud, users with excessive permissions can expand the blast radius of an attack, leaving organizations open to all sorts of malicious activity."

FDA, CISA warn of cybersecurity vulnerabilities affecting Illumina Universal Copy Service

Source: https://industrialcyber.co/medical/fda-cisa-warn-of-cybersecurity-vulnerabilities-affecting-illumina-universal-copy-service/

From the Article: "The U.S. Department of Health & Human Services (HHS) Food and Drug Administration (FDA) and the Cybersecurity Infrastructure Security Agency (CISA) have published separate advisories regarding a remotely exploitable, low-complexity attack vulnerability in Illumina Universal Copy Service (UCS) equipment, which is deployed globally by the healthcare and public health sector."

WordPress Plugin "Appointment and Event Booking Calendar for WordPress - Amelia" vulnerable to cross-site scripting

Source: https://jvn.jp/en/jp/JVN00971105/

From the Article: "WordPress Plugin "Appointment and Event Booking Calendar for WordPress - Amelia" contains a cross-site scripting vulnerability."

Phishing Attack Frequency Rises Nearly 50% as Some Sectors Increase by as Much as 576%

Source: https://blog.knowbe4.com/phishing-attack-frequency-rises

From the Article: "New data provides a multi-faceted look at the changing face of phishing

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

attacks. This data includes who's being targeted, the tactics being used, and why phishing attacks continue to work."

WiFi Penetration Testing Cheatsheet for Ethical Hackers

Source: https://latesthackingnews.com/2023/04/30/wifi-penetration-testing-cheatsheet-for-ethical-hackers/

From the Article: "Welcome to the ultimate WiFi penetration testing cheatsheet, an essential resource for every ethical hacker."

HiddenAds Adware Target Android Via Minecraft App Clones

Source: https://latesthackingnews.com/2023/05/01/hiddenads-adware-target-android-via-minecraft-app-clones/

From the Article: "According to a detailed McAfee report, around 38 gaming apps are actively distributing the HiddenAds adware, targeting Android users. These apps even appeared on the Google Play Store, luring even those gamers who stick to downloading from official sources only."

Multiple Vulnerabilities Spotted In APC Easy UPS Software

Source: https://latesthackingnews.com/2023/05/01/multiple-vulnerabilities-spotted-in-apc-easy-ups-software/

From the Article: "Specifically, two of these vulnerabilities could allow remote code execution attacks from an adversary. Whereas a third vulnerability could let the attacker induce denial of service on the target devices."

EV Charging Station Applications – a Growing Cyber Security Risk

Source: https://blog.radware.com/security/2023/05/ev_charging_station_cyber_threats/

From the Article: "EV applications usually interact with each other and third-party services and platforms via APIs or JavaScript plugins. These applications process both sensitive, personal driver information and information about the vehicle."

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

Legal firm HWL Ebsworth suffers Russian cyber attack: client, employee data stolen

Source: https://dsf.newscorpaustralia.com/theaustralian/subscription/

From the Article: "No cancellations during the first 12 months. Each payment, once made, is non-refundable, subject to law. A valid active email address and Australian mobile phone number are required for account set up. Not in conjunction with any other offer. "

Hackers use fake 'Windows Update' guides to target Ukrainian govt - Bleeping Computer

Source: https://www.bleepingcomputer.com/news/security/hackers-use-fake-windows-update-guides-to-target-ukrainian-govt/

From the Article: "The Computer Emergency Response Team of Ukraine (CERT-UA) says Russian hackers are targeting various government bodies in the country with malicious emails supposedly containing instructions on how to update Windows as a defense against cyber attacks."

Nashua NH schools open Monday despite cyber-attack - WMUR

Source: https://www.wmur.com/article/nashua-schools-cyber-attack-ransomware-5123/43754889

From the Article: "Schools were open Monday in Nashua while the district continued to deal with what officials called a sophisticated cyberattack.The director of communications for the school district said the system was hit by a ransomware attack, but she couldn't say what demands, if any, have been made."

Gateway Casinos Ontario Begin Reopening Following Cyberattack - Casino.org

Source: https://www.casino.org/news/gateway-casinos-ontario-begin-reopening-following-cyberattack/

From the Article: "Gateway Casinos over the weekend began reopening some of its properties in Ontario roughly two weeks after a cyberattack forced the Canadian gaming firm to shutter most of its operations in the province."

Clop, LockBit Leveraging 3 Known Vulnerabilities in Healthcare Ransomware Attacks, HHS Warns

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

Source: https://healthitsecurity.com/news/clop-lockbit-leveraging-3-known-vulnerabilities-in-healthcare-ransomware-attacks-hhs-warns

From the Article: "The Health Sector Cybersecurity Coordination Center (HC3) issued a sector alert about the current operations of Clop and LockBit ransomware groups. The Ransomware-as-a-Service (RaaS) groups have recently been leveraging three known vulnerabilities (CVE-2023-27351, CVE-2023-27350, and CVE-2023-0669) to target healthcare organizations."

Organisations still fall victim to ransomware despite being prepared: Report - ITP.net

Source: https://www.itp.net/security/organisations-still-fall-victim-to-ransomware-despite-being-prepared-report

From the Article: "Four out of the five top challenges to stopping ransomware were people or process related, according to Fortinet."

Massachusetts health plan hit with ransomware and service disruptions

Source: https://www.healthcareitnews.com/news/massachusetts-health-plan-hit-ransomware-and-service-disruptions

From the Article: "As a result of a ransomware attack affecting Harvard Pilgrim Health Care commercial and Medicare Advantage Stride plans, HPHC parent company Point32Health says it is waiving prior authorizations for most medical and behavioral health-covered services and cannot accept claim submissions for Harvard Pilgrim commercial members at this time."

Report shows nearly 600% annual growth in vulnerable cloud attack surface

Source: https://www.securitymagazine.com/articles/99276-report-shows-nearly-600-annual-growth-in-vulnerable-cloud-attack-surface

From the Article: "A new report reveals security organizations experienced 133% year-over-year growth in cyber assets, resulting in increased security complexity and mounting pressure for cloud enterprises."

Thales Threat Report - 50% of Firms Not Ready for Ransomware - BankInfoSecurity

Source: https://www.bankinfosecurity.com/thales-data-threat-report-key-findings-todd-

Link back to Table of Contents

moore-rsa-a-21893

From the Article: "Now in its 10th year, the Thales Data Threat Report outlines and quantifies the key threats faced by the global cybersecurity industry. Ransomware continues to be a growing threat but, surprisingly, more than half of respondents have no defense plan in place, said Todd Moore, vice president of encryption products at Thales Cloud Protection and Licensing."

FBI director asks for millions to catch up with China's cyber mischief

Source: https://interestingengineering.com/culture/fbi-director-asks-for-millions-catch-up-with-chinas-cyber-mischief

From the Article: "Christopher Wray, director of the Federal Bureau of Investigation, revealed this surprising fact while speaking at the House Appropriations Committee's subcommittee on Commerce, Justice, Science, and Related Agencies."

Key U.S. Marshals computers still down 10 weeks after breach - DataBreaches.net

Source: https://www.databreaches.net/key-u-s-marshals-computers-still-down-10-weeks-after-breach/

From the Article: "A key law enforcement computer network has been down for 10 weeks, the victim of a ransomware attack that has frustrated efforts by senior officials to get the system back up and running — raising concerns about how to secure critical crime-fighting operations."

HC3: Ransomware Groups are Exploiting GoAnywhere and PaperCut Vulnerabilities

Source: https://www.hipaajournal.com/hc3-ransomware-groups-are-exploiting-goanywhere-and-papercut-vulnerabilities/

From the Article: "The Health Sector Cybersecurity and Coordination Center (HC3) has issued a fresh ransomware warning to the healthcare and public health (HPH) sector following a spate of attacks on the HPH sector in April by the Clop and LockBit ransomware groups."

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

Veeam backup hacked, DOJ SolarWinds discovery, Americold frozen out - CISO Series

Source: https://cisoseries.com/veeam-backup-hacked-doj-solarwinds-discovery-americold-frozen-out/

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."

Newark's Ultralife takes financial hit in first quarter due to ransomware attack

Source: https://www.fingerlakes1.com/2023/05/01/newarks-ultralife-takes-financial-hit-in-first-quarter-due-to-ransomware-attack/

From the Article: "Ultralife Corp. announced last week that a cybersecurity ransomware attack earlier this year has affected the company's first quarter financial results. The attack targeted their Newark, Wayne County, and Virginia Beach, Va. facilities and was discovered on January 25, with the company disclosing the attack on March 2."

Leaders from government and industry participate in sessions on ransomware, cyber strategy

Source: https://insidecybersecurity.com/daily-news/week-ahead-leaders-government-and-industry-participate-sessions-ransomware-cyber-strategy

From the Article: "Key industry groups are hosting senior cybersecurity officials at events on countering ransomware and the national cyber strategy, while NIST focuses on supply chain and small-business security needs in webinars this week."

Restaurants Under Attack from Cybercriminals: How to Protect Your Business

Source: https://modernrestaurantmanagement.com/restaurants-under-attack-from-cybercriminals-how-to-protect-your-business/

From the Article: "As the restaurant industry becomes more reliant on technology, the risk of cyber attacks is rising. Cybercriminals are increasingly targeting restaurants, seeking to steal sensitive customer data and disrupt business operations. One study found that in 2016, the food and beverage industry accounted for ten percent of all data breaches. "

Link back to Table of Contents

Global cyber-attacks continue to rise in Q1 2023 - Digit.fyi

Source: https://www.digit.fyi/global-cyber-attacks-continue-to-rise-in-q1-2023/

From the Article: "Global weekly attacks rose by 7% in Q1 2023 versus the same quarter last year, with organisations facing an average of 1248 attacks per week, according to a new report by Check Point Research (CPR)."

Hackers selling new malware on Telegram that targets macOS users - IBTimes India

Source: https://www.ibtimes.co.in/hackers-selling-new-malware-telegram-that-targets-macos-users-858696

From the Article: "Threat actors are selling a new malware called -- Atomic macOS Stealer (AMOS) on the Telegram channel to target macOS platforms, which is capable of extracting autofill information, passwords, wallets, and more."

New Research Shows Ransomware Attacks Resurge with Victims Doubling in 2023

Source: https://securitytoday.com/articles/2023/05/01/new-research-shows-ransomware-attacks-resurge-with-victims-doubling-in-2023.aspx

From the Article: "Black Kite, provider third-party cyber risk intelligence, recently released its highly anticipated report, “Ransomware Threat Landscape 2023: Ransomware Resurgence”. The report provides a comprehensive analysis of 2,708 ransomware victims with detailed insights into attacks from April 2022 to March 2023.."

Sophos: Hackers utilize LOLbins to attack organizations - Back End News

Source: https://backendnews.net/sophos-hackers-utilize-lolbins-to-attack-organizations/

From the Article: "Among the 500 unique tools and techniques that many cyberattackers are using, Sophos’ research found “Living off the Land” binaries (LOLBins) are among the most used these days."

Link back to Table of Contents

After Ransomware Attack, Aiims Pushes For Maintaining Cyber Hygiene - CNBCTV18.com

Source: https://www.cnbctv18.com/technology/after-ransomware-attack-aiims-pushes-for-maintaining-cyber-hygiene-16537771.htm

From the Article: "Months after a cyber attack crippled medical services for many weeks at country's premiere medical institute, the All India Institute of Medical Sciences (AIIMS), last week issued a standard operating procedure (SoP) for all of it's medical staff including doctors, officials regarding use of pen drives."

China has 50 hackers for every FBI cyber agent, says Bureau boss - The Register

Source: https://www.theregister.com/2023/05/01/fbi_director_wray_china_testimony/

From the Article: "Speaking at the House Appropriations Committee's subcommittee on Commerce, Justice, Science, and Related Agencies, director Christopher Wray tried to justify the Bureau's budget request by outlining the threats it is trying to counter."

What does ChatGPT know about phishing?

Source: https://securelist.com/chatgpt-anti-phishing/109590/

From the Article: "Hearing all the buzz about the amazing applications of ChatGPT and other language models, our team could not help but ask this question. We work on applying machine learning technologies to cybersecurity tasks, specifically models that analyze websites to detect threats such as phishing."

German IT provider Bitmarck hit by cyberattack

Source: https://securityaffairs.com/145568/hacking/bitmarck-cyberattack.html

From the Article: "The German IT service provider Bitmarck announced on April 30 it had taken all its systems offline due to a cyberattack. The incident impacted statutory health insurance companies that have their IT operated by BITMARCK. The company immediately reported the incident to the responsible authorities."

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

Iranian govt uses BouldSpy Android malware for internal surveillance operations

Source: https://securityaffairs.com/145550/hacking/iran-bouldspy-android-spyware.html

From the Article: "Researchers at the Lookout Threat Lab have discovered a new Android surveillance spyware, dubbed BouldSpy, that was used by the Law Enforcement Command of the Islamic Republic of Iran (FARAJA)."

Russian APT Nomadic Octopus hacked Tajikistani carrier

Source: https://securityaffairs.com/145536/apt/nomadic-octopus-targets-tajikistani-carrier.html

From the Article: "Russian cyber espionage group Nomadic Octopus (aka DustSquad) has hacked a Tajikistani telecoms provider to spy on 18 entities, including high-ranking government officials, telecommunication services, and public service infrastructures."

How Morris Worm Command and Control Changed Cybersecurity

Source: https://securityintelligence.com/articles/how-morris-worm-changed-cybersecurity/

From the Article: "A successful cyberattack requires more than just gaining entry into a victim's network. To truly reap the rewards, attackers must maintain a persistent presence within the system. After establishing communication with other compromised network devices, actors can stealthily extract valuable data. The key to all this is a well-developed Command and Control (C2 or C&C) infrastructure."

'BouldSpy' Android Malware Used in Iranian Government Surveillance Operations

Source: https://www.securityweek.com/bouldspy-android-malware-used-in-iranian-government-surveillance-operations/

From the Article: "The Iranian government has been using the BouldSpy Android malware to spy on minorities and traffickers."

Tenable Cyber Watch: 3 Hot Takes from RSA Conference, Samsung Employees Leak

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

Sensitive Data to ChatGPT, and more

Source: https://www.tenable.com/blog/tenable-cyber-watch-3-hot-takes-from-rsa-conference-samsung-employees-leak-sensitive-data-to

From the Article: "This week's edition of the Tenable Cyber Watch dishes out 3 hot takes from the RSA Conference and unpacks the Samsung employee data leak to ChatGPT. Also covered: What cyber professionals say is their biggest worry."

Biomedical device vulnerability. Ransomware and the US Marshals. US DoJ emphasizes disruption. Updates on the hybrid war. OT risk-sharing.

Source: https://thecyberwire.com/newsletters/daily-briefing/12/83

From the Article: "FDA warns of vulnerability affecting biomedical devices. Ransomware's effects continue to trouble US Marshals Service fugitive tracking. US Justice Department shifts to disruption and prevention of large scale cybercrime. Fresh phish from the GRU. ETHOS: a new private-sector OT risk information-sharing platform."

Cybersecurity in space: not as far out as you'd think.

Source: https://thecyberwire.com/stories/b4e997c1d2364e1180242df611d9c2a7/cybersecurity-in-space-not-as-far-out-as-youd-think

From the Article: "After lots of behind-the-scenes work, I'm so glad (and relieved!) that I can now talk about T-Minus, our new daily space industry podcast at N2K Space, which I have the privilege of hosting."

Google Blocks 1.43 Million Malicious Apps, Bans 173,000 Bad Accounts in 2022

Source: https://thehackernews.com/2023/05/google-blocks-143-million-malicious.html

From the Article: "Google disclosed that its improved security features and app review processes helped it block 1.43 million bad apps from being published to the Play Store in 2022."

Link back to Table of Contents

Vietnamese Threat Actor Infects 500,000 Devices Using 'Malverposting' Tactics

Source: https://thehackernews.com/2023/05/vietnamese-threat-actor-infects-500000.html

From the Article: "A Vietnamese threat actor has been attributed as behind a "malverposting" campaign on social media platforms to infect over 500,000 devices worldwide over the past three months to deliver variants of information stealers such as S1deload Stealer and SYS01stealer."

APT28 Targets Ukrainian Government Entities with Fake "Windows Update" Emails

Source: https://thehackernews.com/2023/05/apt28-targets-ukrainian-government.html

From the Article: "The Computer Emergency Response Team of Ukraine (CERT-UA) has warned of cyber attacks perpetrated by Russian nation-state hackers targeting various government bodies in the country."

Attackers Use Containers for Profit via TrafficStealer

Source: https://www.trendmicro.com/en_us/research/23/d/attackers-use-containers-for-profit-via-trafficstealer.html

From the Article: "We found TrafficStealer abusing open container APIs in order to redirect traffic to specific websites and manipulate engagement with ads."

AI Adoption Slow For Design Tools

Source: https://semiengineering.com/slow-ai-adoption-within-eda/

From the Article: "While ML adoption is robust, full AI is slow to catch fire. But that could change in the future."

Anomali Cyber Watch: APT37 Adopts LNK Files, Charming Kitten Uses BellaCiao Implant-Dropper, ViperSoftX Infostealer Unique Byte Remapping Encryption

Source: https://www.anomali.com/blog/anomali-cyber-watch-apt37-adopts-lnk-files-

Link back to Table of Contents

charming-kitten-uses-bellaciao-implant-dropper-vipersoftx-infostealer-unique-byte-remapping-encryption

From the Article: "The various threat intelligence stories in this iteration of the Anomali Cyber Watch discuss the following topics: APT, Byte remapping, Cloud C2s, Infostealers, Iran, North Korea, RATs, and Vulnerabilities."

Fake Websites Impersonating Association To ChatGPT Poses High Risk, Warns Check Point Research

Source: https://blog.checkpoint.com/research/fake-websites-impersonating-association-to-chatgpt-poses-high-risk-warns-check-point-research/

From the Article: " Check Point Research (CPR) sees a surge in malware distributed through websites appearing to be related to ChatGPT Since the beginning of 2023, 1 out of 25 new ChatGPT-related domain was either malicious or potentially malicious."

Chain Reaction: ROKRAT's Missing Link

Source: https://research.checkpoint.com/2023/chain-reaction-rokrats-missing-link/

From the Article: "ROKRAT has not changed significantly over the years, but its deployment methods have evolved, now utilizing archives containing LNK files that initiate multi-stage infection chains."

Adobe ColdFusion Unauthenticated Remote Code Execution

Source: https://packetstormsecurity.com/files/172079/adobe_coldfusion_rce_cve_2023_26360.rb.txt

From the Article: "This Metasploit module exploits a remote unauthenticated deserialization of untrusted data vulnerability in Adobe ColdFusion 2021 Update 5 and earlier as well as ColdFusion 2018 Update 15 and earlier, in order to gain remote code execution."

Link back to Table of Contents

Mobile Mouse 3.6.0.4 Remote Code Execution

Source: https://packetstormsecurity.com/files/172071/mobilemouse3604v2-exec.txt

From the Article: "Mobile Mouse version 3.6.0.4 suffers from a remote code execution vulnerability. This exploit is a second version from the original author of the original exploit released in September of 2022."

Hackers Attack Ukrainian Government With Phony "Windows Update" Guides

Source: https://cyberintelmag.com/attacks-data-breaches/hackers-attack-ukrainian-government-with-phony-windows-update-guides/

From the Article: "According to the Computer Emergency Response Team of Ukraine (CERT-UA), fraudulent emails purporting to give instructions on how to upgrade Windows as a protection against cyberattacks are being sent to various government organizations in the nation by Russian hackers."

Microsoft says Iranian hackers combine influence ops with hacking for maximum impact

Source: https://cyberscoop.com/iranian-information-operations-hacking-microsoft-report/

From the Article: "Iranian state-aligned hackers are increasingly deploying information operations to amplify cyberattacks and gain maximum exposure for their efforts to support the regime's agenda in the Middle East and against Western targets, Microsoft's Digital Threats Analysis Center said Tuesday."

Hacktivism and the new age of cyber warfare

Source: https://www.cybertalk.org/2023/05/02/hacktivism-and-the-new-age-of-cyber-warfare/

From the Article: "Hacktivism has traditionally been associated with loosely managed underground cyber criminal entities. These decentralized and unstructured groups are typically composed of individuals cooperating in support of specific agendas."

Microsoft's next-level nomenclature, naming hacking groups

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

Source: https://www.cybertalk.org/2023/05/01/microsofts-next-level-nomenclature-naming-hacking-groups/

From the Article: "Last week, Microsoft's cyber security division announced that it is changing its taxonomy for naming hacking groups. Previously, Microsoft assigned cyber criminal organizations the names of chemical elements, as listed in the periodic table. "

SLP Vulnerability Exposes Devices to Powerful DDoS Attacks

Source: https://www.cysecurity.news/2023/05/slp-vulnerability-exposes-devices-to.html

From the Article: "Security researchers have recently discovered a new vulnerability that has the potential to launch devastating Distributed Denial of Service (DDoS) attacks."

Defending Against Adversarial Attacks in Machine Learning: Techniques and Strategies

Source: https://www.cysecurity.news/2023/05/defending-against-adversarial-attacks.html

From the Article: "As machine learning algorithms become increasingly prevalent in our daily lives, the need for secure and reliable models is more important than ever. "

The Threat of Deepfakes: Hacking Humans

Source: https://www.cysecurity.news/2023/05/the-threat-of-deepfakes-hacking-humans.html

From the Article: "Deepfake technology has been around for a few years, but its potential to harm individuals and organizations is becoming increasingly clear. In particular, deepfakes are becoming an increasingly popular tool for hackers and fraudsters looking to manipulate people into giving up sensitive information or making financial transactions."

Illumina: FDA, CISA Warns Against Security Flaw Making Medical Devices Vulnerable to Remote Hacking

Source: https://www.cysecurity.news/2023/05/illumina-fda-cisa-warns-against.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 US Government has issued a warning for healthcare providers and lab employees against a critical flaw, discovered in the genomics giant Illumina's medical devices, used by threat actors to alter or steal sensitive patient medical data."

Atomic macOS Malware: New Malware Steals Credit Card Credentials in Chrome

Source: https://www.cysecurity.news/2023/05/atomic-macos-malware-new-malware-steals.html

From the Article: "A brand-new malware has apparently been targeting macOS. The malware, according to BleepingComputer, is named "Atomic" and was being sold to cybercriminals in darknet markets for $1,000 a month. "

China 'Innovated' Its Cyberattack Tradecraft, Mandia Says

Source: https://www.darkreading.com/attacks-breaches/china-innovated-its-cyberattack-tradecraft-mandia-says

From the Article: "Mandiant CEO Kevin Mandia explains why a recently revealed targeted attack by a cyber-espionage group out of China rivals the SolarWinds attack in its complexity, and weighs in on how defenders can best leverage generative AI."

FBI Focuses on Cybersecurity With $90M Budget Request

Source: https://www.darkreading.com/remote-workforce/fbi-focuses-cybersecurity-90m-budget-request

From the Article: "Never before has cyber been higher on the FBI's list of priorities."

APT28 Employs Windows Update Lures to Trick Ukrainian Targets

Source: https://www.darkreading.com/attacks-breaches/apt28-employs-windows-update-lures-to-trick-ukrainian-targets

From the Article: "The phishing emails were sent using names of system administrators and a letter containing instructions to protect against hackers."

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

Labor to appoint dedicated privacy commissioner to combat data breaches

Source: https://www.theguardian.com/world/2023/may/02/labor-to-appoint-dedicated-privacy-commissioner-to-combat-data-breaches

From the Article: "The federal government will appoint a dedicated privacy commissioner to deal with the increasing threat of data breaches, the attorney general has announced."

Australian law firm HWL Ebsworth hit by Russian-linked ransomware attack

Source: https://www.theguardian.com/technology/2023/may/02/australian-law-firm-hwl-ebsworth-hit-by-russian-linked-ransomware-attack

From the Article: "Late last week, the ALPHV/Blackcat ransomware group posted on its website that 4TB of company data had been hacked, including employee CVs, IDs, financial reports, accounting data, client documentation, credit card information, and a complete network map."

Packet Storm New Exploits For April, 2023

Source: https://packetstormsecurity.com/files/172080/202304-exploits.tgz

From the Article: "This archive contains all of the 195 exploits added to Packet Storm in April, 2023."

CompanyMaps 8.0 Cross Site Scripting

Source: https://packetstormsecurity.com/files/172075/cmaps80-xss.txt

From the Article: "CompanyMaps version 8.0 suffers from a persistent cross site scripting vulnerability."

AC Repair And Services 1.0 SQL Injection

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

Source: https://packetstormsecurity.com/files/172070/acrepairservices10-sql.txt

From the Article: "AC Repair and Services version 1.0 suffers from a remote SQL injection vulnerability."

Android Device Migration Tools Bug Let Hackers Steal App Data & Login to Your Accounts

Source: https://gbhackers.com/android-device-migration-tools-flaw-let-hackers-steal/

From the Article: "Smartphones are frequently replaced by users when newer versions of smartphones with much more features are released. The exchange of smartphones has a significant complication in transferring data to the new device."

AresLoader Malware Attacking Citrix Users Through Malicious GitLab Repo

Source: https://gbhackers.com/aresloader-malware-attacking-citrix-users/

From the Article: "Cyble Research and Intelligence Labs (CRIL) has recently detected AresLoader, a novel loader that is found to be disseminating numerous malware families."

Google Blocked Over 1.4 Million Malicious Apps From Google Play Store

Source: https://gbhackers.com/google-blocked-1-4-million-apps/

From the Article: "Since Google bought Android 2005, its sole responsibility has been to provide the best user experience and ensure security for its users. Google Play Protect was installed on every Android device to ensure every application was secure."

Google and Apple lead initiative for an industry specification to address unwanted tracking

Source: http://security.googleblog.com/2023/05/google-and-apple-lead-initiative-for.html

From the Article: "Today Google and Apple jointly submitted a proposed industry specification to help combat the misuse of Bluetooth location-tracking devices for

unwanted tracking."

Medusa ransomware gang leaks students' psychological reports and abuse allegations

Source: https://www.bitdefender.com/blog/hotforsecurity/medusa-ransomware-gang-leaks-students-psychological-reports-and-abuse-allegations/

From the Article: "Students and teachers at the Minneapolis Public School (MPS) District, which suffered a huge ransomware attack< at the end of February, have had highly sensitive information about themselves published on the web, including allegations of abuse by teachers and psychological reports."

Cyberpress Launches Cybersecurity Press Release Distribution Platform

Source: https://www.hackread.com/cyberpress-launches-cybersecurity-press-release-distribution-platform/

From the Article: "Cybersecurity gets a new dedicated newswire. Cyberpress, a press release distribution platform for the cybersecurity industry, has opened its doors today. This newswire service provides an effective communications approach for cybersecurity companies, public relations agencies and marketing advisors, investment firms operating in the space and more."

Insider Threat: Organizations Must Focus on Risk

Source: https://www.bankinfosecurity.com/insider-threat-organizations-must-focus-on-risk-aspect-a-21942

From the Article: "The definition of insider threat seems to have evolved since the hybrid workforce became the norm. More organizations are now talking about the "compromised insider." Randall Trzeciak of Software Engineering Institute said that in the last three years, insider threats have changed to insider risks."

Patient in Leaked Photos Drops Pursuit for Ransom Payment

Source: https://www.bankinfosecurity.com/patient-in-leaked-photos-drops-pursuit-for-ransom-payment-a-21941

Link back to Table of Contents

From the Article: "A woman suing Lehigh Valley Health Network dropped her push for a court order requiring the medical center to pay ransomware hackers in exchange for their pledge to remove from the dark web partially naked exam room photos stolen during a hacking incident."

Killer Use Cases for AI Dominate RSA Conference Discussions

Source: https://www.bankinfosecurity.com/blogs/killer-use-cases-for-ai-dominate-rsa-conference-discussions-p-3442

From the Article: "And it happened: Discussions at this year's RSA conference again and again came back to generative artificial intelligence - but with a twist."

Easily exploitable flaw in Oracle Opera could spell trouble for hotel chains (CVE-2023-21932)

Source: https://www.helpnetsecurity.com/2023/05/02/cve-2023-21932/

From the Article: "A recently patched vulnerability (CVE-2023-21932) in Oracle Opera, a property management system widely used in large hotel and resort chains, is more critical than Oracle says it is and could be easily exploited by unauthenticated remote attackers to access sensitive information, a group of researchers has warned."

Fake ChatGPT desktop client steals Chrome login data

Source: https://www.helpnetsecurity.com/2023/05/02/chatgpt-infostealer/

From the Article: "Researchers are warning about an infostealer mimicking a ChatGPT Windows desktop client that's capable of copying saved credentials from the Google Chrome login data folder."

Conceal collaborates with Moruga to help organizations detect malicious activity

Source: https://www.helpnetsecurity.com/2023/05/03/conceal-moruga/

From the Article: "Conceal announced partnership with Moruga to help organizations of

all sizes monitor and detect malicious activity at the edge. Moruga's proprietary Cybhermetics security platform aggregates industry-leading cybersecurity companies to create the Zero Day Protection Suite. "

The costly threat that many businesses fail to address

Source: https://www.helpnetsecurity.com/2023/05/02/insider-attacks-damage/

From the Article: "Insider attacks such as fraud, sabotage, and data theft plague 71% of U.S. businesses, according to Capterra. These schemes can cost companies hundreds of thousands of dollars and the vast majority of businesses (79%) say they take longer to uncover than external threats."

Why the manufacturing sector needs stronger cyber defenses

Source: https://www.helpnetsecurity.com/2023/05/02/manufacturing-sector-cyberattacks/

From the Article: "In this Help Net Security interview, Filipe Beato, Lead, Centre for Cybersecurity, World Economic Forum, shares his expertise on the correlation between the digitization of the manufacturing sector and the rise in cyberattacks."

Hacker steals Bitcoins from Russia, destroys them or donates them to Ukraine

Source: https://news.hitb.org/content/hacker-steals-bitcoins-russia-destroys-them-or-donates-them-ukraine

From the Article: "A mysterious bitcoiner appears to have weaponized the Bitcoin blockchain against the Russian state by exposing hundreds of wallets allegedly held by security agencies, according to crypto tracing firm Chainalysis."

At RSA Conference 2023, tales of real-world cyberattacks and warnings of fearsome new threats

Source: https://news.hitb.org/content/rsa-conference-2023-tales-real-world-cyberattacks-and-warnings-fearsome-new-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.

From the Article: "The challenges of securing organizations haven't changed much in the past year, and that means there's still a lot more that needs to be done — especially as generative artificial intelligence and chatbots will require new tactics to fight attackers."

New SPARTA v1.3 framework offers significant updates covering space cyber threats

Source: https://industrialcyber.co/regulation-standards-and-compliance/new-sparta-v1-3-framework-offers-significant-updates-covering-space-cyber-threats/

From the Article: "The Aerospace Corporation released last week v1.3 of its Space Attack Research and Tactic Analysis (SPARTA) framework, providing a general information page, SPARTA navigator, and SPARTA Matrix Updates. The latest version also delivers 14 new countermeasures (CMs) and includes SPARTA Countermeasure Mapper."

HC3 issues fresh sector alert warning of data breaches from Cl0p, Lockbit ransomware groups

Source: https://industrialcyber.co/medical/hc3-issues-fresh-sector-alert-warning-of-data-breaches-from-cl0p-lockbit-ransomware-groups/

From the Article: "The Health Sector Cybersecurity Coordination Center (HC3) at the U.S. Department of Health & Human Services (HHS) once again issued a fresh sector alert on Friday, warning companies about two ransomware-as-a-service (RaaS) groups, Cl0p and Lockbit. "

Homeland Security Committee hears Jen Easterly on current cybersecurity posture in defending critical infrastructure

Source: https://industrialcyber.co/cisa/homeland-security-committee-hears-jen-easterly-on-current-cybersecurity-posture-in-defending-critical-infrastructure/

From the Article: "The U.S. Homeland Security Committee hosted a subcommittee hearing last week as it works on evaluating the President's Fiscal Year 2024 budget request. The meeting comes as the U.S. Cybersecurity and Infrastructure Security Agency (CISA) has requested US$3.1 billion, a $145 million increase over the FY 23 enacted funding level. "

Link back to Table of Contents

Hackers Take Advantage Of TBK DVR Camera System's Severe Flaws

Source: https://informationsecuritybuzz.com/hackers-take-advantage-of-tbk-dvr-camera-systems-flaws/

From the Article: "The alert notes that the fact that there are tens of thousands of TBK DVRs available under several brands, publicly accessible PoC code, and an easy-to-exploit make this issue an attractive target for attackers."

UK Gun Owners May Be Targeted After Rifle Association Breach

Source: https://www.infosecurity-magazine.com/news/gun-owners-targeted-rifle/

From the Article: "Unknown number of members compromised in cyber-attack."

Bitmarck Halts Operations Due to Cybersecurity Breach

Source: https://www.infosecurity-magazine.com/news/bitmarck-halts-operations/

From the Article: "Bitmarck does not believe customer data was impacted due to the breach."

South Korean Lures Used to Deploy ROKRAT Malware

Source: https://www.infosecurity-magazine.com/news/south-korean-lures-deploy-rokrat/

From the Article: "This shift is not exclusive to ROKRAT but represents a larger trend that became popular in 2022."

Hackers Exploit High Severity Flaw in TBK DVR Camera System

Source: https://www.infosecurity-magazine.com/news/high-severity-flaw-tbk-dvr-camera/

From the Article: "Vulnerability derives from an error the camera experiences when handling a maliciously crafted HTTP cookie."

Link back to Table of Contents

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

Phishing as an Espionage Tactic for Cybercriminals

Source: https://blog.knowbe4.com/phishing-espionage-tactic

From the Article: "Phishing is a familiar criminal tactic. It's also used by intelligence services for cyber espionage campaigns. On Friday, April 28th, 2023, CERT-UA, Ukraine's Computer Emergency Response Team, reported that Russian operators are sending phishing emails that misrepresent themselves as sending instructions on installing a Windows security update."

Critical Vulnerabilities Spotted In Zyxel Firewall

Source: https://latesthackingnews.com/2023/05/02/critical-vulnerabilities-spotted-in-zyxel-firewall/

From the Article: "Heads up, Zyxel users! The vendors have patched a few critical vulnerabilities in Zyxel Firewall that could allow remote command execution attacks. Users must rush to update their devices with the latest software releases to receive the patches."

Cisco Patched Known Vulnerability In IP Phone 7800 And 8800 Series

Source: https://latesthackingnews.com/2023/05/01/cisco-patched-known-vulnerability-in-ip-phone-7800-and-8800-series/

From the Article: "As explained, the vulnerability specifically affected the Cisco Discovery Protocol processing feature of the Cisco IP Phones. The bug appeared due to insufficient input validation of the incoming Cisco Discovery Protocol packets."

Apple delivers first-ever Rapid Security Response "cyberattack" patch – leaves some users confused

Source: https://nakedsecurity.sophos.com/2023/05/01/apple-delivers-first-ever-rapid-security-response-cyberattack-patch-leaves-some-users-confused/

From the Article: "Our approach has therefore been simply to assume the worst, and to

infer that the story that Apple wasn't telling ran something like this: "Devices analysed in the wild found to have hidden spyware implanted by unknown threat actors.""

US Marshals to Unveil 'Fully Reconstituted System' Following Ransomware Attack

Source: https://www.nextgov.com/cybersecurity/2023/05/us-marshals-unveil-fully-reconstituted-system-following-ransomware-attack/385866/

From the Article: "Offline since February, the new system will have improved cybersecurity countermeasures."

Sensitive Data Is Being Leaked From Servers Running Salesforce Software

Source: https://arstechnica.com/information-technology/2023/04/misconfigured-servers-running-salesforce-software-are-leaking-sensitive-data/

From the Article: "Servers running software sold by Salesforce are leaking sensitive data managed by government agencies, banks, and other organizations, according to a post published Friday by KrebsOnSecurity."

Cyber-Attack Sparks Fears That Criminals Could Target UK Gun Owners

Source: https://www.theguardian.com/technology/2023/apr/29/cyber-attack-sparks-fears-that-criminals-could-target-uk-gun-owners-for-firearms

From the Article: "Police are investigating a cyber-attack involving potentially thousands of British gun owners, raising concerns that organised criminals may target them for firearms."

High Severity SLP Bug Could Launch Amplified DoS Attacks

Source: https://www.scmagazine.com/news/network-security/high-severity-slp-bug-amplified-dos-attacks

From the Article: "A high-severity vulnerability in the internet's legacy Service Location Protocol (SLP) could let attackers spoof User Datagram Protocol (UDP) traffic to conduct significantly amplified denial-of-service (DoS) attacks."

Link back to Table of Contents

Proofpoint Unveils New Innovations to Combat Increasingly Common Threats

Source: https://mytechdecisions.com/network-security/proofpoint-unveils-new-innovations-to-combat-increasingly-common-threats/

From the Article: "Ahead of the 2023 RSA Conference, Proofpoint, Inc., the Sunnyvale, Calif.-based cybersecurity and compliance company, unveiled a host of innovations across its Aegis Threat Protection, Identity Threat Defense and Sigma Information Protection platforms. The company's latest solutions empower organizations to stop malicious email attacks, detect and prevent identity-based threats and defend sensitive data from theft, loss and insider threats."

Data loss costs go up, and not just from ransom shakedowns • The Register - TheRegister.

Source: https://www.theregister.com/2023/05/02/data_breach_costs_rise/

From the Article: "Data loss – particularly from ransomware attacks – has always been a costly proposition for enterprises. However, the price organizations have to pay is going up, not only in terms of the ransom demanded but also for the cost of investigating attacks and the lawsuits that increasingly follow in the wake of such breaches."

Mayor: Nashua ransomware attack confined to school district records | Local News

Source: https://www.unionleader.com/news/local/mayor-nashua-ransomware-attack-confined-to-school-district-records/article_5d67c1fb-13fa-538f-925d-ea2406bc976c.html

From the Article: "The "sophisticated cyberattack" that infiltrated school district records over the weekend was limited to the district's IT system, and investigators have determined that no other city departments have been targeted, Mayor Jim Donchess said Tuesday afternoon."

Local restaurants fully back online after ransomware attack - Laconia Daily Sun

Source: https://www.laconiadailysun.com/news/local/local-restaurants-fully-back-online-after-ransomware-attack/article_ab620934-e918-11ed-a99c-67e05980eda9.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: "Great NH Restaurants, which owns nine eateries across the state, including T-Bones and Cactus Jack's in Laconia, shared a statement Monday that a ransomware issue preventing use of its rewards and gift card programs had been resolved."

Problems continue from Spartanburg Co. ransomware attack - WSPA

Source: https://www.wspa.com/news/local-news/problems-continue-from-spartanburg-co-ransomware-attack/

From the Article: "Difficulties caused by last week's ransomware attack continued at Spartanburg County offices Tuesday. Computer systems at the sheriff's office, the county courthouse, and the Register of Deeds offices remain offline."

Carrington reports ransomware attack at tech vendor - National Mortgage News

Source: https://www.nationalmortgagenews.com/news/carrington-mortgage-reports-ransomware-data-breach

From the Article: "A ransomware attack at a technology firm compromised information of Carrington Mortgage Services customers including partial Social Security numbers, the servicer said last week."

Ransomware Containment Company BullWall Enters North American Market - MSSP Alert

Source: https://www.msspalert.com/cybersecurity-services-and-products/ransomware-containment-company-bullwall-enters-north-american-market/

From the Article: "North American organizations can use BullWall's solution to monitor file shares, application servers and database servers in cloud and data center environments, the company said in a prepared statement. That way, these organizations can prevent server data encryption and block attempts to encrypt and exfiltrate data."

Report: Ransomware Attacks on Schools Increased in Q1 2023 - Government Technology

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

Source: https://www.govtech.com/education/k-12/report-ransomware-attacks-on-schools-increased-in-q1-2023

From the Article: "Ransomware attacks on schools and other public institutions rose sharply in the past six months, according to a Virginia-based cybersecurity company that monitors worldwide activity on a quarterly basis."

Is legislation the best defence against ransomware attacks? - Raconteur

Source: https://www.raconteur.net/risk-regulation/is-legislation-the-best-defence-against-ransomware-attacks/

From the Article: "Even as it was winding down last year, the infamous Russian-based gang behind the Conti ransomware mounted successful attacks on Costa Rica's public institutions in a bid to foment a popular uprising. The government of President Rodrigo Chaves refused to pay up, but it had to declare a state of emergency to deal with the fallout. "

Data Leakage Becoming Bigger Issue For Chipmakers

Source: https://semiengineering.com/data-leakage-becoming-bigger-issue-for-chipmakers/

From the Article: "Increasing complexity, disaggregation, and continued feature shrinks add to problem; oversight is scant."

ML Automotive Chip Design Takes Off

Source: https://semiengineering.com/ml-automotive-chip-design-takes-off/

From the Article: "Tools utilize reinforcement learning for a variety of applications, including developing AI chips."

Role Of IoT Software Expanding

Source: https://semiengineering.com/role-of-iot-software-expanding/

Link back to Table of Contents
The articles have been 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: "Software is becoming more critical and complex, and it is becoming central to design and security."

Microelectronics Funding Surge Shows Onshoring Progress

Source: https://www.nationaldefensemagazine.org/articles/2023/4/26/microelectronics-funding-surge-shows-onshoring-progress

From the Article: "A recent surge in microelectronics funding from the Defense Department includes a hefty sum directed to dual-use technology, expanding a pool of opportunity for both the department and its suppliers, a recent report said."

Government CHIPS on the table: How higher DOD microelectronics funding is here to stay

Source: https://www.mckinsey.com/industries/aerospace-and-defense/our-insights/government-chips-on-the-table-how-higher-dod-microelectronics-funding-is-here-to-stay

From the Article: "New US Department of Defense funding for microelectronics R&D gives semiconductor companies an opportunity—but manufacturers and designers must adapt to meet it."

Defense industry reports improving post-COVID supply chain

Source: https://www.defensenews.com/industry/2023/04/28/defense-industry-reports-improving-post-covid-supply-chain/

From the Article: "WASHINGTON — More than three years after the COVID pandemic began to upend supply chains around the world, some defense executives say they are starting to see signs of recovery. But supply delays and shortfalls are still posing serious challenges to some major programs."

What's Holding Up the US Military's Use of AI?

Source: https://www.nextgov.com/emerging-tech/2023/04/dods-frontline-ai-adoption-still-limited-network-and-data-collection/385732/

Link back to Table of Contents

The articles have been 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: "Two of the obstacles are spotty networks and inadequate data, CENTCOM's CTO says."

DoD and European Defence Agency sign cooperation pact in support of shared military interests

Source: https://breakingdefense.com/2023/04/dod-and-european-defence-agency-sign-cooperation-pact-in-support-of-shared-military-interests/

From the Article: "The pact was inked in Brussels on Wednesday by William LaPlante, under secretary of defense for acquisition and sustainment and Jiři Šedivý, EDA chief executive."

DoD and European Defence Agency sign cooperation pact in support of shared military interests

Source: https://breakingdefense.com/2023/04/dod-and-european-defence-agency-sign-cooperation-pact-in-support-of-shared-military-interests/

From the Article: "The pact was inked in Brussels on Wednesday by William LaPlante, under secretary of defense for acquisition and sustainment and Jiři Šedivý, EDA chief executive."

Risk of war with China over Taiwan is real, intel leaders warn

Source: https://www.washingtontimes.com/news/2023/may/4/risk-war-china-over-taiwan-real-intel-leaders-warn/

From the Article: "Beijing threat takes center stage in annual Senate briefing"

Taiwan PCB makers face challenges relocating production to Southeast Asia

Source: https://www.digitimes.com/news/a20230502PD221/taiwan-pcb-manufacturing-production-relocation-thailand.html

From the Article: "Taiwan-based PCB manufacturers are facing challenges as they push

forward with relocating production to Southeast Asia, particularly Thailand, such as limited land, water, and electrical supplies, according to industry sources."

Counterfeit Parts Risk Reduced with Nearshoring - EE Times

Source: https://www.eetimes.com/nearshoring-mitigates-counterfeit-component-risks/

From the Article: "Nearshoring also helps to increase quality control. With operations taking place closer to home, manufacturers can more easily monitor the quality of the components and ensure that they meet the required specifications."

Global Semiconductor Sales Decrease 8.7% in First Quarter; March Sales Tick Up Month-to-Month for First Time Since May 2022

Source: https://www.semiconductors.org/global-semiconductor-sales-decrease-8-7-in-first-quarter-march-sales-tick-up-month-to-month-for-first-time-since-may-2022/?utm_content=246988618&utm_medium=social&utm_source=linkedin&hss_channel=lcp-1940570

From the Article: "WASHINGTON—May 1, 2023—The Semiconductor Industry Association (SIA) today announced worldwide sales of semiconductors totaled $119.5 billion during the first quarter of 2023, a decrease of 8.7% compared to the fourth quarter of 2022 and 21.3% less than the first quarter of 2022."

Readout of Deputy Secretary of Defense Dr. Kathleen Hicks' Round Table Meeting With U.S. B

Source: https://www.defense.gov/News/Releases/Release/Article/3378684/readout-of-deputy-secretary-of-defense-dr-kathleen-hicks-round-table-meeting-wi/

From the Article: "Deputy Secretary of Defense Dr. Kathleen Hicks held a meeting with executives from six U.S. lithium-ion battery and critical mineral companies today at the Pentagon to communicate the Department's focus on growing the U.S. battery industry, while reducing supply chain vulnerabilities caused by over-reliance on overseas competitors. "

Packagist Repository Hacked: Over a Dozen PHP Packages with 500 Million

Link back to Table of Contents

Compromised

Source: https://thehackernews.com/2023/05/packagist-repository-hacked-over-dozen.html

From the Article: "PHP software package repository Packagist revealed that an "attacker" gained access to four inactive accounts on the platform to hijack over a dozen packages with over 500 million installs to date."

Copter crashes raise questions on control rod in gearbox 504859

Source: https://www.tribuneindia.com/news/nation/copter-crashes-raise-questions-on-control-rod-in-gearbox-504859

From the Article: "The crash of an Advanced Light Helicopter (ALH) near Kishtwar, Jammu and Kashmir, has again raised questions on metallurgical issues with a critical component, the control rod, on board the copter."

The undersea tech industry has a responsibility to develop the next generation workforce - The Boston Globe

Source: https://www.bostonglobe.com/2023/05/01/metro/undersea-tech-industry-has-responsibility-develop-next-generation-workforce/

From the Article: "The tech industry must commit to being involved with developing the next generation workforce through strong and dedicated partnerships with K-12 and higher education institutions. A concerted effort needs to be focused on building a diverse future workforce that ensures opportunity for all, and that all communities are fully represented."

Semi foundation launches workforce development menu to support chips act funding applications

Source: https://www.semi.org/en/blogs/technology-and-trends/semi-foundation-launches-workforce-development-menu-to-support-chips-act-funding-applications

From the Article: "NIST requires comprehensive workforce development plans that outline partnerships, equity strategies, demonstrated commitments to Good Jobs Principles, support services for training participants, metrics and milestones, and –

Link back to Table of Contents

probably most controversially – plans for providing childcare in all applications valued at $150 million and above."

Researchers Discover 3 Vulnerabilities in Microsoft Azure API Management Service

Source: https://thehackernews.com/2023/05/researchers-discover-3-vulnerabilities.html

From the Article: "Three new security flaws have been disclosed in Microsoft Azure API Management service that could be abused by malicious actors to gain access to sensitive information or backend services."

Google "We Have No Moat, And Neither Does OpenAI"

Source: https://www.semianalysis.com/p/google-we-have-no-moat-and-neither

From the Article: "Leaked Internal Google Document Claims Open Source AI Will Outcompete Google and OpenAI"

Fleckpe Android Malware Sneaks onto Google Play Store with Over 620,000 Downloads

Source: https://thehackernews.com/2023/05/fleckpe-android-malware-sneaks-onto.html

From the Article: "A new Android subscription malware named Fleckpe has been unearthed on the Google Play Store, amassing more than 620,000 downloads in total since 2022."

Microsoft's Chief Scientific Officer, one of the world's leading A.I. experts, doesn't think a 6 month pause will fix A.I.—but has some ideas of how to safeguard it

Source: https://finance.yahoo.com/news/microsoft-chief-scientific-officer-one-230000103.html

From the Article: "It's now, perhaps more than ever, that underlying philosophical questions rarely mentioned in the workplace are bubbling to the C-Suite: What sets humans apart from machines? What is intelligence—how do you define it? Large language models are getting smarter, more creative, and more powerful faster than we can blink. And, of course, they are getting more dangerous."

Link back to Table of Contents

Worldwide silicon wafer shipments decline in q1 2023 semi reports

Source: https://www.semi.org/en/news-media-press-releases/semi-press-releases/worldwide-silicon-wafer-shipments-decline-in-q1-2023-semi-reports

From the Article: "MILPITAS, Calif. — May 2, 2023 — Worldwide silicon wafer shipments slipped 9.0% quarter-over-quarter to 3,265 million square inches in the first quarter of 2023 and 11.3% from the 3,679 million square inches recorded during the same quarter last year, the SEMI Silicon Manufacturers Group (SMG) reported today in its quarterly analysis of the silicon wafer industry."

Blueprint released for nation's first national semiconductor technology center

Source: https://www.troyrecord.com/2023/04/28/blueprint-released-for-nations-first-national-semiconductor-technology-center

From the Article: "WASHINGTON — U.S. Senate Majority Leader Chuck Schumer recently revealed the U.S. Department of Commerce released additional guidance for the launch of the National Semiconductor Technology Center (NSTC), created in his CHIPS and Science Act."

N. Korean Kimsuky Hackers Using New Recon Tool ReconShark in Latest Cyberattacks

Source: https://thehackernews.com/2023/05/n-korean-kimsuky-hackers-using-new.html

From the Article: "The North Korean state-sponsored threat actor known as Kimsuky has been discovered using a new reconnaissance tool called ReconShark as part of an ongoing global campaign."

The US DOD has invented a wearable that quickly identifies infections

Source: https://interestingengineering.com/innovation/the-us-dod-wearable-identifies-infections

From the Article: "The U.S. Department of Defense (DOD) invented a wearable during the pandemic that was extremely adept at identifying infections. "

Link back to Table of Contents
The articles have been 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 Hacker Group Earth Longzhi Resurfaces with Advanced Malware Tactics

Source: https://thehackernews.com/2023/05/chinese-hacker-group-earth-longzhi.html

From the Article: "A Chinese state-sponsored hacking outfit has resurfaced with a new campaign targeting government, healthcare, technology, and manufacturing entities based in Taiwan, Thailand, the Philippines, and Fiji after more than six months of no activity."

ChatGPT Wrote my Code

Source: https://www.linkedin.com/pulse/chatgpt-wrote-my-code-john-cole/

From the Article: "TLDR: There's a major disruption underway and your job may be at risk. What really floored me was GitHub CoPilot."

The Devastating Business Impacts of a Cyber Breach

Source: https://hbr.org/2023/05/the-devastating-business-impacts-of-a-cyber-breach

From the Article: "Cybersecurity risks are becoming more systematic and more severe. Although the short-term impacts of a cyberattack on a business are quite severe, the long-term impacts can be even more important, such as the loss of competitive advantage, reduction in credit rating, and increase in cyber insurance premiums."

Impact Nano, chip materials startup, wins funding from Intel, Goldman Sachs

Source: https://www.reuters.com/markets/us/impact-nano-chip-materials-startup-wins-funding-intel-goldman-sachs-2023-05-04/

From the Article: "OAKLAND, California, May 4 (Reuters) - Impact Nano, a Massachusetts-based startup that makes specialty chemicals for the semiconductor industry and others, said on Thursday it raised $32 million in funding from investors including Intel Capital and Goldman Sachs Asset Management."

Link back to Table of Contents
The articles have been 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 04/28/2023-05/04/2023

Source: https://www.allthingssupplychain.com/supply-chain-weekly-wrap-up-04-28-2023-05-04-2023/

From the Article: "Apple sales fall but iPhone demand persists Apple sales have continued to fall, as the economy slows and buyers, squeezed by rising prices, put off purchases of computers and iPads."

The cost of crime and corruption on Pacific fisheries

Source: https://www.lowyinstitute.org/the-interpreter/cost-crime-corruption-pacific-fisheries

From the Article: "The need for a well-funded response to illegal, unreported and unregulated fishing has never been greater."

North Korean Kimsuky Hacking Group Ups Their Game with New 'ReconShark' Malware

Source: https://www.blackhatethicalhacking.com/news/north-korean-kimsuky-hacking-group-ups-their-game-with-new-reconshark-malware/

From the Article: "The North Korean Kimsuky hacking group has recently been observed using a new version of its reconnaissance malware, dubbed 'ReconShark,' in an expanded cyberespionage campaign targeting organizations across the globe."

APT hacking group uses double DLL sideloading to bypass security

Source: https://www.blackhatethicalhacking.com/news/apt-hacking-group-uses-double-dll-sideloading-to-bypass-security/

From the Article: "An APT hacking group, known as "Dragon Breath," "Golden Eye Dog," or "APT-Q-27," is demonstrating a new trend of using complex variations of the classic DLL sideloading technique to evade detection."

Multiple Vulnerabilities in Google Chrome Could Allow for Arbitrary Code Execution

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

Source: https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-google-chrome-could-allow-for-arbitrary-code-execution_2023-046

From the Article: "Multiple vulnerabilities have been discovered in Google Chrome, the most severe of which could allow for arbitrary code execution. Google Chrome is a web browser used to access the internet. Successful exploitation of the most severe of these vulnerabilities could allow for arbitrary code execution in the context of the logged on user. "

FluHorse – Check Point Research Exposes Newly Discovered Malware Disguised as Legitimate and Popular Android Apps Targeting East Asia

Source: https://blog.checkpoint.com/security/fluhorse-check-point-research-exposes-a-newly-discovered-malware-disguised-as-east-asian-legitimate-popular-android-apps/

From the Article: "Highlights Check Point Research (CPR) uncovered a fresh strain of malware that is cleverly disguised as popular Android applications from East Asia. The malware campaign is highly sophisticated and is directed at a variety of sectors in Eastern Asia."

Check Point Software Applauds U.S. Senators for Investigating Use of AI to Create Malicious Phishing Emails with the IRS

Source: https://blog.checkpoint.com/security/check-point-software-applauds-u-s-senators-for-investigating-use-of-ai-to-create-malicious-phishing-emails-with-the-irs/

From the Article: "This week, United States Senators Maggie Hassan (D-NH), Chuck Grassley (R-IA), Ron Wyden (D-OR), and James Lankford (R-OK), raised their concerns over the potential use of artificial intelligence (AI) to create malicious phishing emails designed to trick Americans into sharing their personal financial information."

Raspberry Robin: Anti-Evasion How-To & Exploit Analysis

Source: https://research.checkpoint.com/2023/raspberry-robin-anti-evasion-how-to-exploit-analysis/

From the Article: "During the last year, Raspberry Robin has evolved to be one of the most distributed malware currently active. During this time, it is likely to be used by many actors to distribute their own malware such as IcedID, Clop ransomware and

more."

Threat Source newsletter (May 4, 2023) — Recapping the biggest headlines to come out of RSA

Source: https://blog.talosintelligence.com/threat-source-newsletter-may-4-2023-recapping-the-biggest-headlines-to-come-out-of-rsa/

From the Article: "I didn't attend the RSA Conference in person, and on top of that, I was at the NFL Draft while the conference was going on. I'm behind on the biggest talks, panels and presentations that came out during the annual security conference, so I've spent the past few days catching up on what seems like the major talking points last week in San Francisco."

TSMC growing presence in EV sector

Source: https://www.digitimes.com/news/a20230504PD211/tsmc-ic-manufacturing-electric-vehicles-automotive-ic.html

From the Article: "The pure-play foundry embraces a three-prong strategy for its automotive business. It is directly teaming up with international automakers to obtain long-term supply agreements, developing new and special manufacturing processes for making automotive chips, and building overseas joint-venture fabs with automotive component makers, the sources said."

China suppliers land 6-inch SiC orders from automotive IDMs, tier-1 suppliers

Source: https://www.digitimes.com/news/a20230504PD215/china-6-inch-silicon-carbide-automotive-ic-news-sic.html

From the Article: "Chinese silicon carbide (SiC) companies including SICC and TankeBlue Semiconductor have secured contracts to supply 6-inch SiC materials to international automotive IDMs and tier-one suppliers, according to industry sources."

China to account for most automotive LiDAR shipment in 2023, DIGITIMES Research says

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

Source: https://www.digitimes.com/news/a20230505VL203/digitimes-research-lidar-adas-china-meet-the-analyst.html&chid=2

From the Article: "LiDAR is rising to be the emerging component differentiating car models in China. According to Evan Chen, an analyst with DIGITIMES Research, global automotive LiDAR shipment is expected to reach 500,000 units in 2023, with China taking up at least 80% of it."

AUO chair sees recovery in China consumer market

Source: https://www.digitimes.com/news/a20230504PD208/auo-china-consumer-market-china-ict-manufacturing-paul-peng.html

From the Article: "Paul Peng, chairman of both LCD panel producer AU Optronics (AUO) and the Taipei Computer Association (TCA), believes the Chinese consumer market is on the mend."

Global smartphone shipments remain in a slump, says Omdia

Source: https://www.digitimes.com/news/a20230505VL208/2023-global-smartphone-demand-inventory.html

From the Article: "Worldwide smartphone shipments totaled 268.5 million units in the first quarter of 2023, according to the latest Omdia smartphone preliminary shipment report. Compared to the previous year, this marks a decrease of 12.7%, and compared to the previous..."

India smartphone shipment declined 16% in 1Q23, Xiaomi saw more than 40% fall

Source: https://www.digitimes.com/news/a20230505VL201/1q23-india-smartphone.html

From the Article: "According to IDC's latest market tracker, due to weak consumer demand, uncertain macroeconomic conditions, and high inventory levels, smartphone shipments in India declined by 16% year-on-year to 31 million units in the first quarter of 2023, the lowest first-quarter record in four years."

Supply Chain Weekly Wrap-Up 04/28/2023-05/04/2023

Link back to Table of Contents

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

Source: https://www.allthingssupplychain.com/supply-chain-weekly-wrap-up-04-28-2023-05-04-2023/

From the Article: "Apple sales fall but iPhone demand persists Apple sales have continued to fall, as the economy slows and buyers, squeezed by rising prices, put off purchases of computers and iPads."

The cost of crime and corruption on Pacific fisheries

Source: https://www.lowyinstitute.org/the-interpreter/cost-crime-corruption-pacific-fisheries

From the Article: "The need for a well-funded response to illegal, unreported and unregulated fishing has never been greater."

North Korean Kimsuky Hacking Group Ups Their Game with New 'ReconShark' Malware

Source: https://www.blackhatethicalhacking.com/news/north-korean-kimsuky-hacking-group-ups-their-game-with-new-reconshark-malware/

From the Article: "The North Korean Kimsuky hacking group has recently been observed using a new version of its reconnaissance malware, dubbed 'ReconShark,' in an expanded cyberespionage campaign targeting organizations across the globe."

APT hacking group uses double DLL sideloading to bypass security

Source: https://www.blackhatethicalhacking.com/news/apt-hacking-group-uses-double-dll-sideloading-to-bypass-security/

From the Article: "An APT hacking group, known as "Dragon Breath," "Golden Eye Dog," or "APT-Q-27," is demonstrating a new trend of using complex variations of the classic DLL sideloading technique to evade detection."

Multiple Vulnerabilities in Google Chrome Could Allow for Arbitrary Code Execution

Source: https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-google-chrome-could-allow-for-arbitrary-code-execution_2023-046

Link back to Table of Contents

The articles have been 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: "Multiple vulnerabilities have been discovered in Google Chrome, the most severe of which could allow for arbitrary code execution. Google Chrome is a web browser used to access the internet. Successful exploitation of the most severe of these vulnerabilities could allow for arbitrary code execution in the context of the logged on user. "

FluHorse – Check Point Research Exposes Newly Discovered Malware Disguised as Legitimate and Popular Android Apps Targeting East Asia

Source: https://blog.checkpoint.com/security/fluhorse-check-point-research-exposes-a-newly-discovered-malware-disguised-as-east-asian-legitimate-popular-android-apps/

From the Article: "Highlights Check Point Research (CPR) uncovered a fresh strain of malware that is cleverly disguised as popular Android applications from East Asia. The malware campaign is highly sophisticated and is directed at a variety of sectors in Eastern Asia."

Raspberry Robin: Anti-Evasion How-To & Exploit Analysis

Source: https://research.checkpoint.com/2023/raspberry-robin-anti-evasion-how-to-exploit-analysis/

From the Article: "During the last year, Raspberry Robin has evolved to be one of the most distributed malware currently active. During this time, it is likely to be used by many actors to distribute their own malware such as IcedID, Clop ransomware and more."

Threat Source newsletter (May 4, 2023) — Recapping the biggest headlines to come out of RSA

Source: https://blog.talosintelligence.com/threat-source-newsletter-may-4-2023-recapping-the-biggest-headlines-to-come-out-of-rsa/

From the Article: "I didn't attend the RSA Conference in person, and on top of that, I was at the NFL Draft while the conference was going on. I'm behind on the biggest talks, panels and presentations that came out during the annual security conference, so I've spent the past few days catching up on what seems like the major talking points last week in San Francisco."

Link back to Table of Contents

TSMC growing presence in EV sector

Source: https://www.digitimes.com/news/a20230504PD211/tsmc-ic-manufacturing-electric-vehicles-automotive-ic.html

From the Article: "The pure-play foundry embraces a three-prong strategy for its automotive business. It is directly teaming up with international automakers to obtain long-term supply agreements, developing new and special manufacturing processes for making automotive chips, and building overseas joint-venture fabs with automotive component makers, the sources said."

China suppliers land 6-inch SiC orders from automotive IDMs, tier-1 suppliers

Source: https://www.digitimes.com/news/a20230504PD215/china-6-inch-silicon-carbide-automotive-ic-news-sic.html

From the Article: "Chinese silicon carbide (SiC) companies including SICC and TankeBlue Semiconductor have secured contracts to supply 6-inch SiC materials to international automotive IDMs and tier-one suppliers, according to industry sources."

China to account for most automotive LiDAR shipment in 2023, DIGITIMES Research says

Source: https://www.digitimes.com/news/a20230505VL203/digitimes-research-lidar-adas-china-meet-the-analyst.html&chid=2

From the Article: "LiDAR is rising to be the emerging component differentiating car models in China. According to Evan Chen, an analyst with DIGITIMES Research, global automotive LiDAR shipment is expected to reach 500,000 units in 2023, with China taking up at least 80% of it."

AUO chair sees recovery in China consumer market

Source: https://www.digitimes.com/news/a20230504PD208/auo-china-consumer-market-china-ict-manufacturing-paul-peng.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: "Paul Peng, chairman of both LCD panel producer AU Optronics (AUO) and the Taipei Computer Association (TCA), believes the Chinese consumer market is on the mend."

Global smartphone shipments remain in a slump, says Omdia

Source: https://www.digitimes.com/news/a20230505VL208/2023-global-smartphone-demand-inventory.html

From the Article: "Worldwide smartphone shipments totaled 268.5 million units in the first quarter of 2023, according to the latest Omdia smartphone preliminary shipment report. Compared to the previous year, this marks a decrease of 12.7%, and compared to the previous..."

India smartphone shipment declined 16% in 1Q23, Xiaomi saw more than 40% fall

Source: https://www.digitimes.com/news/a20230505VL201/1q23-india-smartphone.html

From the Article: "According to IDC's latest market tracker, due to weak consumer demand, uncertain macroeconomic conditions, and high inventory levels, smartphone shipments in India declined by 16% year-on-year to 31 million units in the first quarter of 2023, the lowest first-quarter record in four years."

Smartphone AP shipments to China expected to pick up 10% on quarter in 2Q23, says DIGITIMES Research

Source: https://www.digitimes.com/news/a20230505VL207/digitimes-research-mobile-components-smartphone.html

From the Article: "Looking into second-quarter 2023, smartphone AP shipments to China-based vendors are estimated to come to 132 million units, increasing 10% sequentially as smartphone brands ramp up their inventory more aggressively than they did in the prior quarter to prepare for the 618 shopping festival in China."

EV price war in China may herald industrial shakeup

Source: https://www.digitimes.com/news/a20230505VL202/china-industrial-price-

vehicle.html&chid=10

From the Article: "As companies engage in an EV price war amid an end to subsidies and expected slower growth, experts believe China's EV industry will experience a shakeup in which smaller brands may be wiped out of the market."

ChatGPT creates automotive OS dilemma for automakers

Source: https://www.digitimes.com/news/a20230504PD203/nvidia-automotive-chatgpt.html

From the Article: "The generative AI revolution brought about by ChatGPT also includes future cars. Current focus points include the new business opportunities created by in-vehicle AI through smart cockpits and human-vehicle interactions and generative AI's assistance..."

Server demand outlook remains promising

Source: https://www.digitimes.com/news/a20230504PD212/ai-server-aws-cloud-data-center-cloud-server-llm-public-cloud-server-demand-server.html

From the Article: "According to sources in the server industry, inventory corrections are likely to persist in the short term but the long-term outlook remains promising."

AIGC wave prompts major Chinese internet companies to speed chip development

Source: https://www.digitimes.com/news/a20230505PD200/ai-chips-aigc-alibaba-baidu-meituan-tencent.html

From the Article: "With the rise of AI-generated content (AIGC) in 2023, major players in the tech sector are joining the ranks of AI chip manufacturing one after another. Not only are international corporations like Amazon, Microsoft, and Google joining the AI chip race,..."

AP Memory to expand AI memory biz

Source: https://www.digitimes.com/news/a20230504PD218/ap-memory-business-hpc-

ic-design-distribution.html

From the Article: "AP Memory Technology, which specializes in customized IoT RAM and other DRAM memory, will extend its AI memory business by entering the HPC area, according to company president Wen Chen."

WT Micro expects sales recovery in 2H23

Source: https://www.digitimes.com/news/a20230504PD216/wt-microelectronics-ic-design-distribution-ic-distributor-revenue.html

From the Article: "IC distributor WT Microelectronics expects its revenue to hit bottom for 2023 in the second quarter before growing sequentially in the third and fourth quarters."

Samsung union warns of historic walkout as slump persists

Source: https://www.digitimes.com/news/a20230504VL212/samsung-labor-union-ic-manufacturing-chips+components.html

From the Article: "Samsung Electronics Co. faces its first-ever labor strike after an influential union threatened to stage a walkout to protest wages and the company's alleged attempts to block labor organization."

Taiwan 'CHIPS Act' enters countdown for finalization

Source: https://www.digitimes.com/news/a20230502PD218/taiwan-chips-act-tax-incentive-ic-manufacturing-research-and-development-semiconductor-equipment.html

From the Article: "After consulting with the Ministry of Finance (MOF), the MOEA proposed certain thresholds for companies hoping to apply for the tax incentives, including a minimum annual spend of NT$6 billion (US$194.68 million) in R&D, R&D must account for at least 6% of annual sales, and a minimum spend of NT$10 billion on equipment used for advanced process manufacturing."

Costly sub-3nm investments challenging TSMC, others

Link back to Table of Contents

Source: https://www.digitimes.com/news/a20230502PD220/tsmc-3nm-capex-foundry-ic-manufacturing.html

From the Article: "The high cost of manufacturing processes smaller than 3nm and related investments is posing a challenge to TSMC and its Korean and US peers, who are attempting to maintain adequate long-term margins and profits, according to industry sources."

TSMC overseas foundry quotes to be 10-30% higher than in Taiwan

Source: https://www.digitimes.com/news/a20230502PD200/tsmc-arizona-foundry-ic-manufacturing.html

From the Article: "TSMC has begun to formulate pricing strategies for its new overseas wafer fabs. Quotes for advanced chips to be fabricated by its plant in Arizona are estimated to be 20-30% higher than corresponding prices in Taiwan, while mature process chips from..."

Instagram sugar daddy reportedly arrest

Source: https://cybernews.com/news/instagram-sugar-daddy-reportedly-arrest/

From the Article: "Brazilian police have reportedly arrested Victor Mendes – the alleged scammer behind the sugar daddy scam designed to con gullible victims on Instagram."

Invasion could cost world economy US$1tn - Taipei Times

Source: https://www.taipeitimes.com/News/front/archives/2023/05/06/2003799247

From the Article: "CHIP SHUTDOWN: US intelligence officials expressed different views on China at a hearing, ranging from little threat of a Taiwan invasion to an attack as early as 2025"

US senators pitch Taiwan tax plan to spur chip ventures - Taipei Times

Source: https://www.taipeitimes.com/News/front/archives/2023/05/06/2003799249

Link back to Table of Contents

From the Article: "Such an agreement would allow the US and Taiwan to stop double taxing businesses that operate in each place. Double taxation has become a major sticking point in US efforts to attract Taiwanese investment in semiconductors and other high-tech goods, with Taiwan saying the costs are too high."

Retired officer guilty of recruiting spies for China - Taipei Times

Source: https://www.taipeitimes.com/News/taiwan/archives/2023/05/06/2003799257

From the Article: "SPIES LIKE US: Shao Wei-chiang had recruited at least two people, including a former army colonel who was in February sentenced to seven-and-a-half years in prison"

Great China Fund raises concern over TSMC returns - Taipei Times

Source: https://www.taipeitimes.com/News/biz/archives/2023/05/06/2003799227

From the Article: "DECLINE IN EFFICIENCY: Uni-President Asset Management Corp's Derek Lin said he invested in E Ink Holdings instead of increasing his fund's stake in the chipmaker"

AI can teach students to be curious - Taipei Times

Source: https://www.taipeitimes.com/News/editorials/archives/2023/05/06/2003799240

From the Article: "We might not realize it, but we rely on artificial intelligence (AI) for our pleasures and distractions. AI algorithms feed us our posts on Facebook, products on Amazon and movies on Netflix. They have become our dopamine "fixes.""

John Deng calls on US to widen chip subsidy rules - Taipei Times

Source: https://www.taipeitimes.com/News/biz/archives/2023/05/06/2003799229

From the Article: "Deng said he he told Raimondo that Taiwanese semiconductor companies would likely face higher investment costs in the US than in Taiwan and that he hoped they would be eligible for financial assistance."

Link back to Table of Contents

Taiwan ideal for chipmakers, US investment: minister - Taipei Times

Source: https://www.taipeitimes.com/News/taiwan/archives/2023/05/05/2003799197

From the Article: "Taiwanese chipmakers would expand production in the US as much as they can afford to do so, Taiwan's chief trade representative said, but added that Taiwan remains an ideal place for semiconductor production, as well as US business and investment, despite tensions with China."

TSMC in talks for 10bn euros chip fab in Germany - Taipei Times

Source: https://www.taipeitimes.com/News/biz/archives/2023/05/04/2003799073

From the Article: "LOOKING TO EUROPE: The facility in Saxony would be a joint venture with Robert Bosch, NXP and Infineon, and is likely to focus on 28-nanometer chips, sources said"

Chipmaker Vanguard delays expansion - Taipei Times

Source: https://www.taipeitimes.com/News/biz/archives/2023/05/04/2003799071

From the Article: "SLOW GOING: While orders from some customers have started to rise, demand from others remains sluggish as inventory digestion continues, the contract chipmaker said"

Four delegations from Japan to visit Taiwan this week - Taipei Times

Source: https://www.taipeitimes.com/News/taiwan/archives/2023/05/03/2003799049

From the Article: "Four delegations that include 18 Japanese lawmakers are scheduled to visit Taiwan this week, Taiwan-Japan Relations Association Secretary-General Fan Chen-kuo (范振國) said yesterday."

Taiwan accelerating shift away from China: official - Taipei Times

Link back to Table of Contents
The articles have been 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.taipeitimes.com/News/front/archives/2023/05/03/2003799030

From the Article: "'RED' AND 'NON-RED': India and Southeast Asia are the main beneficiaries as more Taiwanese manufacturers try to create two separate supply chains, NDC Minister Kung Ming-hsin said"

Taiwan 'Chips act' sets R&D spending at NT$6 billion - Taipei Times

Source: https://www.taipeitimes.com/News/front/archives/2023/05/02/2003798964

From the Article: "TAX BREAKS: Companies at the top of their game that are strategically vital to global supply chains are the prime targets of the new tax program"

Silicon Motion sees gradual recovery in memory market

Source: https://www.digitimes.com/news/a20230505PD206/emmc-silicon-motion-ssd.html

From the Article: "Silicon Motion Technology, a memory device controller IC company, has seen an increase in client orders that may lead to a stronger market rebound by the end of 2023."

EDITORIAL: 'Chip act' only benefits giants - Taipei Times

Source: https://www.taipeitimes.com/News/editorials/archives/2023/05/02/2003798952

From the Article: "The Ministry of Economic Affairs yesterday said that to be eligible for the tax breaks, a company should invest at least NT$10 billion (US$325.31 million) in new, advanced manufacturing equipment every year."

A Chinese occupation would harm the world - Taipei Times

Source: https://www.taipeitimes.com/News/editorials/archives/2023/05/01/2003798902

From the Article: "Today, if Chinese submarines wanted to travel straight to the US' west coast, they would likely travel through the Bashi Channel south of Taiwan, which the US military monitors."

Link back to Table of Contents

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

EDITORIAL: China is losing its economic luster - Taipei Times

Source: https://www.taipeitimes.com/News/editorials/archives/2023/05/01/2003798899

From the Article: "In other words, demand for China's goods is still weak, despite a rebound in overall economic growth that has been driven largely by the services sector following the end of strict COVID-19 restrictions at the end of last year."

Microsoft, AMD join forces on AI chips: sources - Taipei Times

Source: https://www.taipeitimes.com/News/biz/archives/2023/05/06/2003799232

From the Article: "ALTERNATIVE TO NVIDIA: Microsoft is said to offer engineering resources to the chipmaker, which called artificial intelligence its 'No. 1 strategic priority'"

Qualcomm outlook slides on phone slump forecast - Taipei Times

Source: https://www.taipeitimes.com/News/biz/archives/2023/05/05/2003799155

From the Article: "WEAK DEMAND: Chief executive officer Cristiano Amon said there were expectations the China market would bounce back, but those signs have not emerged yet"

Rising demand to gradually boost ChipMOS revenue - Taipei Times

Source: https://www.taipeitimes.com/News/biz/archives/2023/05/05/2003799150

From the Article: "ChipMOS Technologies Inc (南茂科技), a tester and packager of driver ICs and memory chips, yesterday said that revenue would rise gradually from this quarter, aided by significant improvement in demand for its packaging services used in flat panel drive ICs."

China's reopening party over for emerging markets - Taipei Times

Link back to Table of Contents
The articles have been 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.taipeitimes.com/News/biz/archives/2023/05/02/2003798943

From the Article: "UNCERTAINTY: Although China's economy improved over the past two months, investors question whether that growth would continue into the second quarter"

Chip sales set to drop 11.2 percent this year: US report - Taipei Times

Source: https://www.taipeitimes.com/News/biz/archives/2023/05/01/2003798891

From the Article: "CHALLENGES MOUNT: The next decade is to bring stagnating markets for devices while geopolitical tensions and deglobalization sap demand, a research firm said"

Boosting Taiwan, US defense ties - Taipei Times

Source: https://www.taipeitimes.com/News/editorials/archives/2023/05/04/2003799091

From the Article: "The geopolitical situation in the region has created an urgency for defense industrial cooperation between Taiwan and the US. The Chinese People's Liberation Army has extended its "gray-zone operations" by conducting close reconnaissance drone flights around Taiwan's remote islands and outposts, as well as entering the nation's air defense identification zone."

Tech, AI driving job changes for nearly 1/4 of all workers - Taipei Times

Source: https://www.taipeitimes.com/News/biz/archives/2023/05/02/2003798950

From the Article: "LABOR SHIFT: About 75 percent of firms said they expect to adopt new tech that would cut up to 26 million record-keeping and administrative jobs"

Xi Jinping urges China to seize AI opportunities to modernise industry

Source: https://www.scmp.com/tech/tech-war/article/3219623/chinese-leader-xi-jinping-urges-country-seize-opportunities-artificial-intelligence-modernise

From the Article: "On Friday, Xi said China should seize opportunities in AI to build a

‘holistic, advanced, and harm-free’ modern industrial system. At an April 28 Politburo meeting, Chinese leaders concluded that China must ‘pay attention to the development of artificial general intelligence’."

China still a ‘huge market’ for US chip companies despite risks

Source: https://www.scmp.com/tech/policy/article/3219238/china-still-huge-market-us-chip-companies-despite-risks-says-semiconductor-trade-group

From the Article: "The Biden administration is preparing to solicit bids from chip makers that want to manufacturing plants in the US under President Joe Biden’s Chips and Science Act. SIA’s Neuffer said he is optimistic the administration will be pragmatic in dealing with guardrails to make sure the Chips Act is successful and companies can get the funds."

China chip tool makers see windfall from semiconductor investment boom

Source: https://www.scmp.com/tech/big-tech/article/3218899/tech-war-china-chip-tool-makers-see-windfall-semiconductor-investment-boom-amid-us-trade

From the Article: "Suppliers including Naura Technology Group, Advanced Micro-Fabrication Equipment and National Silicon Industry Group see robust demand in China. US sanctions against China’s semiconductor industry have allowed domestic suppliers to become more closely aligned with local foundries’ requirements."

SK Hynix rows back on plans to upgrade chip tech at Wuxi plant: report

Source: https://www.scmp.com/tech/tech-war/article/3219537/tech-war-sk-hynix-halts-plans-upgrade-chip-tech-wuxi-plant-due-pressure-us-sanctions-china-report

From the Article: "SK Hynix’s strategy ‘involves shifting its capacity expansion back to South Korea, while the Wuxi fab caters to domestic demand in China’, report says. If confirmed, move would represent another case where Korean chip makers have reviewed China investments in light of US restrictions."

Qualcomm outlook grim as smartphone sales stay weak

Link back to Table of Contents

Source: https://www.scmp.com/tech/tech-trends/article/3219329/qualcomm-outlook-grim-smartphone-sales-stay-weak

From the Article: "While Qualcomm hopes smartphone sales will recover in China in the second half, CEO Cristiano Amon said ‘we have not seen evidence of meaningful recovery’. Global smartphone shipments fell 13 per cent in the first quarter, according to research firm Canalys."

China slams US Chips Act subsidies at WTO as tensions ratchet higher

Source: https://www.scmp.com/tech/tech-war/article/3219279/tech-war-china-slams-us-chips-act-subsidies-wto-beijings-latest-protest-against-washingtons

From the Article: "The Chips and Science Act, signed into law by President Biden in 2022, sets aside US$53 billion to fund domestic chip production and research. China representative says industry subsidies allow US to ‘interfere with the allocation of market resources’ and show ‘double standards’."

How boom in smart cars has boosted Chinese auto chip makers like Black Sesame

Source: https://www.scmp.com/tech/big-tech/article/3219146/boom-smart-vehicles-drives-chinese-carmakers-and-third-party-producers-black-sesame-ramp-auto-chip

From the Article: "Hemmed in by US sanctions on advanced chips, China has formed an army of producers that are able to churn out mature node chips for use in cars. As take-up of intelligent vehicles continues, chips related to autonomous driving and intelligent cockpits are developing fast."

AI is making scams harder to detect, but cyber firms are fighting back

Source: https://www.scmp.com/tech/article/3219280/generative-ai-chatgpt-will-be-weaponised-scammers-cybersecurity-arms-race-experts-warn

From the Article: "Generative artificial intelligence is allowing scammers to mimic voices, write more sophisticated phishing emails, and create malware. Cybersecurity firms are deploying AI themselves to keep up with rapidly evolving threats."

Link back to Table of Contents

Latest Reshoring Numbers Could Bode Well for Processors

Source: https://www.ptonline.com/articles/latest-reshoring-numbers-could-bode-well-for-processors

From the Article: "Jobs resulting from reshoring and foreign direct investment set record highs in 2022 after doing the same in 2021. "

Reshoring and FDI up 53%, a new record

Source: https://industrialsupplymagazine.com/pages/News-050123-Reshoring-and-FDI-up-53,-a-new-record.php

From the Article: "Reshoring + FDI (foreign direct investments) job announcements in 2022 were at the highest rate ever recorded, according to The Reshoring Initiative's 2022 Data Report. The organization said fourth-quarter announcements accelerated even more than anticipated due to the Chips and Infrastructure Acts and deglobalization trends."

New world order for semiconductors is emerging!

Source: https://pradeepstechpoints.wordpress.com/2023/04/18/new-world-order-for-semiconductors-is-emerging/

From the Article: "CHIPS for America's has had a very strong start! Department of Commerce has received 200 Statements of Interest (SoIs) for semiconductor projects across 35 states, post the notice of funding opportunity (NOFO). DoC is accepting statements on rolling basis."

Portable Devices Fueled the Growth of Power Semiconductor Industry

Source: https://timestech.in/portable-devices-fueled-the-growth-of-power-semiconductor-industry/

From the Article: "Reducing energy loss and increasing their lifespan, semiconductors use silicon carbide (SiC) in wind and solar power converters. Due to its wide band gap, SiC is used in high-power applications."

Link back to Table of Contents

Intel Faces Hurdles in Tower Semiconductor Acquisition - TipRanks.com

Source: https://www.tipranks.com/news/intel-faces-hurdles-in-tower-semiconductor-acquisition

From the Article: "Intel (NASDAQ:INTC) has reportedly engaged in early-stage discussions with China regarding its proposed acquisition of Tower Semiconductor (NASDAQ:TSEM), but approval isn't expected within the next few weeks."

Agreement with Indiana, Purdue and Belgium-based company to expand semiconductor industry

Source: https://www.jconline.com/story/news/local/2023/05/05/semiconductor-industry-to-expand-even-further-with-this-agreement/70182912007/

From the Article: "Purdue University and the state of Indiana entered into a first-of-its-kind agreement with Belgium-based nano and digital technology company, imec, which states its name in the lowercase format."

Samsung Can Overtake TSMC In 5 Years Says Foundry Head

Source: https://wccftech.com/samsung-can-overtake-tsmc-in-5-years-says-foundry-head/

From the Article: "Korean chaebol Samsung Electronics believes it can overcome the Taiwan Semiconductor Manufacturing Company (TSMC) in five years as both firms roll out the next generation 2-nanometer semiconductor manufacturing process."

German chip plant breaks ground in 'major step forward' for EU

Source: https://thenextweb.com/news/german-chip-plant-breaks-ground-semiconductor-industry-infineon

From the Article: "Europe's chip plans are taking shape"

Global semiconductor firm to expand in PH with US$200-M investment pledge

Link back to Table of Contents
The articles have been 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://mb.com.ph/2023/5/3/global-semiconductor-firm-to-expand-in-ph-with-us-200-m-investment-pledge

From the Article: "WASHINGTON, D.C.—A global semiconductor company intends to expand in the Philippines by investing USD 200 million in a new research and development (R&D) facility in Cavite."

TSMC in Advanced Talks to Establish First European Plant in Germany - Best Stocks

Source: https://beststocks.com/tsmc-in-advanced-talks-to-establish-first-eur/

From the Article: "According to recent reports, Taiwan Semiconductor Manufacturing Company (TSMC) is currently in advanced negotiations with suppliers to establish its very first European plant in the city of Dresden, Germany."

Europe must boost chip production amid Asia risks: EU chief

Source: https://techxplore.com/news/2023-05-europe-boost-chip-production-asia.html

From the Article: "Europe must boost mass production of vital semiconductors due to worsening geopolitical risks in Asian chip-making centers, European Commission president Ursula von der Leyen said Tuesday."

Infineon strengthens Europe's semiconductor industry with "Smart Power Fab"

Source: https://www.eenewseurope.com/en/infineon-strengthens-europes-semiconductor-industry-with-smart-power-fab/

From the Article: "On Tuesday, Infineon will break ground with great fanfare for a new semiconductor fab in Dresden. The company intends to expand its production capacity by a good third."

Arizona, Texas attracting EV and chip megafactories

Source: https://www.freightwaves.com/news/arizona-texas-attracting-ev-and-chip-megafactories

Link back to Table of Contents

From the Article: "Inflation Reduction Act has helped states lure electric vehicle and battery companies looking to expand"

Infineon starts building €5 bn semiconductor plant in Dresden - TelecomLead

Source: https://www.telecomlead.com/semiconductor/infineon-starts-building-e5-bn-semiconductor-plant-in-dresden-110186

From the Article: "Infineon Technologies has broken ground for building a new semiconductor plant in Dresden with an investment volume of €5 billion."

GlobalFoundries buys 800 acres needed for second chip fab

Source: https://www.timesunion.com/business/article/global-foundries-buys-800-acres-needed-second-17999993.php

From the Article: "MALTA — GlobalFoundries has completed the purchase of approximately 800 acres adjacent to its chip manufacturing plant, giving the company enough land to eventually build a second chip fab."

Boost promised for advanced chip industry

Source: https://www.koreaherald.com/view.php?ud=20230502000642

From the Article: "Industry Ministry renews commitment to creating new W300tr cluster for advanced AI, automotive chips"

Fukuoka researcher eager to revive Japan-made semiconductors

Source: https://www.japantimes.co.jp/news/2023/05/01/national/kyushu-fukuoka-semiconductors/

From the Article: "The Kyushu Institute of Technology's School of Computer Science and Systems Engineering, located on gently rolling hills in Iizuka, Fukuoka Prefecture, is offering courses for working adults in an effort to revive semiconductor manufacturing in the Kyushu region."

Link back to Table of Contents

Odisha to start program for semiconductor designing and manufacturing

Source: https://kalingatv.com/state/odisha-to-start-program-for-semiconductor-design-and-manufacturing/

From the Article: "The Odisha government will start a swanky facility for semiconductor designing and manufacturing and generate high-end jobs."

New Vulnerability in Popular WordPress Plugin Exposes Over 2 Million Sites to Cyberattacks

Source: https://thehackernews.com/2023/05/new-vulnerability-in-popular-wordpress.html

From the Article: "Users of Advanced Custom Fields plugin for WordPress are being urged to update version 6.1.6 following the discovery of a security flaw."

Dragon Breath APT Group Using Double-Clean-App Technique to Target Gambling Industry

Source: https://thehackernews.com/2023/05/dragon-breath-apt-group-using-double.html

From the Article: "An advanced persistent threat (APT) actor known as Dragon Breath has been observed adding new layers of complexity to its attacks by adopting a novel DLL side-loading mechanism."

OTORIO secures US patent, claims proprietary algorithm will set standard in OT cybersecurity risk management - Industrial Cyber

Source: https://industrialcyber.co/vendor/otorio-secures-us-patent-uses-proprietary-algorithm-to-set-standard-in-ot-cybersecurity-risk-management/?

From the Article: "Industrial cybersecurity vendor OTORIO has secured a patent from the U.S. Patent and Trademark Office (USPTO) for the company's risk management model and attack graph analysis algorithm. The vendor claims the approach sets a new standard in OT (operational technology) cybersecurity risk management."

Link back to Table of Contents
The articles have been 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 New Strategy for Waging the Microchip Tech War

Source: https://www.csis.org/analysis/chinas-new-strategy-waging-microchip-tech-war

From the Article: "Two dates from 2022 seem certain to echo in geopolitical history. The first, Russia's invasion of Ukraine on February 24, hardly needs further explanation. The second is October 7, when the United States government enacted a series of new export control regulations targeting China's artificial intelligence (AI) and semiconductor industries."

Michael Montenes, the owner of M.S. Hi-Tech, pleads guilty in scheme to obtain 1 million in federal contracts

Source: https://www.erai.com/erai_blog/3182/_michael_montenes_the_owner_of_m_s_hi_tech_pleads_guilty_in_scheme_to_obtain_1_million_in_federal_contracts

From the Article: "Michael Montenes, the owner of Hauppauge-based M.S. Hi-Tech, a distributor of electronic components, pleaded guilty to a charge in connection with a scheme to pay more than $18,000 to a Department of Energy procurement officer in exchange for approximately $969,000 in contracts from that department, according to the U.S. Department of Justice."

New SPARTA v1.3 framework offers significant updates covering space cyber threats - Industrial Cyber

Source: https://industrialcyber.co/regulation-standards-and-compliance/new-sparta-v1-3-framework-offers-significant-updates-covering-space-cyber-threats/

From the Article: "The Aerospace Corporation released last week v1.3 of its Space Attack Research and Tactic Analysis (SPARTA) framework, providing a general information page, SPARTA navigator, and SPARTA Matrix Updates. The latest version also delivers 14 new countermeasures (CMs) and includes SPARTA Countermeasure Mapper."

Distributors boost testing as counterfeit risks 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.

Source: https://epsnews.com/2023/05/04/distributors-boost-testing-as-counterfeit-risks-rise/

From the Article: "Demand for component testing has increased significantly during the chip shortage despite costs — as much as $2,000 — and delays that are incurred during the process. Testing is often outsourced and can damage sample devices. But for a portion of the distribution market, test capabilities distinguish them as trusted sources of supply."

An NCIS Agent's Fight Against Counterfeit and Critical Fraudulent Parts In The Military

Source: https://theaviationist.com/2023/05/06/an-ncis-agents-fight-against-counterfeit-and-critical-fraudulent-parts/

From the Article: "We asked a retired NCIS agent about his experience fighting the proliferation of counterfeit and critical fraudulent parts in the U.S. military."

Sustaining a Resilient Joint Force and Defense Ecosystem that Enables Integrated Deterrence Part 1 of 2

Source: https://www.dau.edu/library/defense-atl/blog/SustainingResilientJointForce-Part1

From the Article: "Integrated Deterrence entails working seamlessly across warfighting domains, theaters, the spectrum of conflict, all instruments of U.S. national power, and our network of alliances and partnerships. … To shore up the foundations for integrated deterrence and campaigning, we will act urgently to build enduring advantages across the defense ecosystem."

Does the National Cybersecurity Strategy spell the end of the government market for commercial software? | Federal News Network

Source: https://federalnewsnetwork.com/commentary/2023/05/does-the-national-cybersecurity-strategy-spell-the-end-of-the-government-market-for-commercial-software/

From the Article: "Section 3.3 of the National Cybersecurity Strategy proposes shifting the liability for “insecure” software products and services to “prevent manufacturers and software publishers with market power from fully disclaiming liability by contract and

establish higher standards of care for software in specific high-risk scenarios."

Private 5G might just make you rethink your wireless options

Source: https://www.networkworld.com/article/3695069/private-5g-might-just-make-you-rethink-your-wireless-options.html

From the Article: "Early adopters in academia, manufacturing, and the military have chosen private 5G for its bandwidth, propagation features, and reliability."

Lawmaker and head of NSF warn of delays to funding US tech research

Source: https://www.reuters.com/technology/lawmaker-head-nsf-warn-delays-funding-us-tech-research-2023-05-05/

From the Article: "Santa Clara, California, May 5 (Reuters) - Silicon Valley's U.S. Democratic Representative Ro Khanna and the director of the National Science Foundation (NSF) warned on Friday against delays to funding for U.S. research in the face of surging technology investment by rivals such as China."

5 Critical Controls for ICS and OT Cybersecurity Strategy

Source: https://www.bankinfosecurity.com/robert-lee-rsa-a-21769

From the Article: "Dragos CEO Robert Lee on Why Vulnerability Patching Is Important in IT But Not OT"

The Pentagon's AI Chief Is 'Scared to Death' of ChatGPT

Source: https://www.defenseone.com/technology/2023/05/pentagons-ai-chief-scared-death-chatgpt/385963/

From the Article: "But other defense leaders are more eager to deploy new artificial-intelligence tools."

Link back to Table of Contents

FBI Focuses on Cybersecurity With $90M Budget Request

Source: https://www.darkreading.com/remote-workforce/fbi-focuses-cybersecurity-90m-budget-request

From the Article: "Never before has cyber been higher on the FBI's list of priorities. Will more money allow the feds to make a greater impact?"

Data Privacy in the AI Era: Five Challenges Raising the Stakes for Businesses

Source: https://www.linkedin.com/pulse/data-privacy-ai-era-five-challenges-raising-stakes-debbie-reynolds/

From the Article: "As AI tools like ChatGPT gain popularity, the business world is increasingly captivated by AI capabilities' swift evolution and deployment. However, it is essential for organizations to assess the necessity and benefits of these AI tools for both themselves and their users."

Microsoft detects Iran turning to cyber-enabled influence operations for greater effect - Industrial Cyber

Source: https://industrialcyber.co/ransomware/microsoft-detects-iran-turning-to-cyber-enabled-influence-operations-for-greater-effect/

From the Article: "Microsoft identified that Iran continues to be a significant threat actor, supplementing its traditional cyberattacks with a new playbook, while leveraging cyber-enabled influence operations (IO) to achieve its geopolitical aims. It also covered Iran's attempts at conducting higher-impact cyberattacks against operational technology (OT) environments. "

Quantum computing race explained

Source: https://cybernews.com/editorial/quantum-computing-race-explained/

From the Article: "The World Economic Forum (WEF) published several think pieces this year describing a post-quantum computing world in which the global chasm between developed and underdeveloped populations only grows larger. But could the gloomy forecast be rosier than expected?"

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

Open-source ETHOS platform to improve availability of OT/ICS devices, networks for data sharing, collaboration - Industrial Cyber

Source: https://industrialcyber.co/features/open-source-ethos-platform-to-improve-availability-of-ot-ics-devices-networks-for-data-sharing-collaboration/

From the Article: "With the release of the OT-centric, vendor-agnostic, open-source ETHOS platform, cybersecurity teams and stakeholders can improve industrial process automation and optimize production while reducing operational costs."

Gentoo Linux Security Advisory 202305-18

Source: https://packetstormsecurity.com/files/172125/glsa-202305-18.txt

From the Article: "Gentoo Linux Security Advisory 202305-18 - Multiple vulnerabilities have been found in libsdl2, the worst of which could result in arbitrary code execution. Versions less than 2.26.0 are affected."

Google launches entry-level cybersecurity certificate to teach threat detection skills

Source: https://www.csoonline.com/article/3695575/google-launches-entry-level-cybersecurity-certificate-to-teach-threat-detection-skills.html

From the Article: "Google has announced a new entry-level cybersecurity certificate to teach learners how to identify common risks, threats, and vulnerabilities, as well as the techniques to mitigate them."

Gentoo Linux Security Advisory 202305-02

Source: https://packetstormsecurity.com/files/172101/glsa-202305-02.txt

From the Article: "Gentoo Linux Security Advisory 202305-2 - Multiple vulnerabilities have been found in Python and PyPy, the worst of which could result in arbitrary code execution."

Link back to Table of Contents

Patch manager Action1 to add vulnerability discovery, prioritization

Source: https://www.csoonline.com/article/3695732/patch-manager-action1-to-add-vulnerability-discovery-prioritization.html

From the Article: "Cloud-native, patch-management application provider Action1 is set to add vulnerability discovery and prioritization capabilities to its namesake flagship platform to help businesses stay ahead of software exploits."

Malware disguised as ChatGPT apps are being used to lure victims, Meta says

Source: https://www.csoonline.com/article/3695728/malware-disguised-as-chatgpt-apps-are-being-used-to-lure-victims-meta-says.html

From the Article: "Facebook's parent company, Meta, has issued a warning that hackers are taking advantage of people's interest in ChatGP and other generative AI applications to trick them into installing malware that pretends to provide AI functionality. "

Attacks increasingly use malicious HTML email attachments

Source: https://www.csoonline.com/article/3695075/attacks-increasingly-use-malicious-html-email-attachments.html

From the Article: "Researchers warn that attackers are relying more on malicious HTML files in their attacks, with malicious files now accounting for half of all HTML attachments sent via email."

Samsung bans staff AI use over data leak concerns

Source: https://www.csoonline.com/article/3695170/samsung-bans-staff-ai-use-over-data-leak-concerns.html

From the Article: "Samsung has reportedly banned employee use of generative AI tools like ChatGPT in a bid to stop transmission of sensitive internal data to external servers."

Threat Roundup for April 28 to May 5

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

Source: https://blog.talosintelligence.com/threat-roundup-0428-0505/

From the Article: "Today, Talos is publishing a glimpse into the most prevalent threats we've observed between April 28 and May 5. As with previous roundups, this post isn't meant to be an in-depth analysis. Instead, this post will summarize the threats we've observed by highlighting key behavioral characteristics, indicators of compromise, and discussing how our customers are automatically protected from these threats."

White House unveils AI rules to address safety and privacy

Source: https://www.computerworld.com/article/3695731/white-house-unveils-ai-rules-to-address-safety-and-privacy.html

From the Article: "President Biden's rules are not legally binding, but they do offer guidance and begin a conversation at the national level about real and existential threats posed by generative AI technologies such as ChatGPT."

Weekly Cyber Threat Report, May 1-5, 2023

Source: https://cyberintelmag.com/threat-intelligence/weekly-cyber-threat-report-may-1-5-2023/

From the Article: "This week's good news includes the first "rapid" security updates from Apple being released for iPhones, iPads, and Macs, Google and Apple working together to stop illegal location-tracking devices, a massive worldwide raid of the dark web drug industry securing over 300 arrests, Meta disrupting malware campaign that used ChatGPT as a scam to steal accounts, and much more."

Crypto Exchange Level Finance Hacked After Two Security Assessments

Source: https://cyberintelmag.com/attacks-data-breaches/crypto-exchange-level-finance-hacked-after-two-security-assessments/

From the Article: "Hackers stole 214,000 LVL tokens from the decentralized exchange and exchanged them for 3,345 BNB, which is worth almost $1,000,000, by taking advantage of a Level Finance smart contract weakness."

Link back to Table of Contents

Coming to DEF CON 31: Hacking AI models

Source: https://cyberscoop.com/def-con-red-teaming-ai/

From the Article: "A group of leading artificial intelligence companies in the U.S. committed on Thursday to open their models to red-teaming at this year's DEF CON hacking conference as part of a White House initiative to address the security risks posed by the rapidly advancing technology."

Top US cyber official warns AI may be the 'most powerful weapon of our time'

Source: https://cyberscoop.com/easterly-warning-weapons-artificial-intelligence-chatgpt/

From the Article: "Director of the Cybersecurity and Infrastructure Security Agency Jen Easterly warned that artificial intelligence may be both the most "powerful capability of our time" and the "most powerful weapon of our time.""

Victims' reluctance to report ransomware stymies efforts to curb cyberattacks, say federal officials

Source: https://cyberscoop.com/ransomware-data-task-force-washington/

From the Article: "Two years after a coalition of cybersecurity companies, public sector organizations and federal agencies came together to form the Ransomware Task Force at the nonprofit Institute for Security and Technology, these digital crimes remain an ongoing and serious problem with attacks seemingly increasingly severe."

FTC accuses Facebook of violating privacy agreement, proposes ban on profiting off children's data

Source: https://cyberscoop.com/ftc-facebook-violating-privacy-agreement/

From the Article: "The Federal Trade Commission proposed on Wednesday that Facebook be prohibited from profiting off of data it collects from minors, a move that comes in response to alleged violations of the company's previous agreements with the agency to protect user privacy."

Link back to Table of Contents

Will the EU's new cyber security law change the game?

Source: https://www.cybertalk.org/2023/05/05/will-the-eus-new-cyber-security-law-change-the-game/

From the Article: "Last month, the European Commission presented a proposal for the EU Law on Cyber Solidarity, a €billion plan intended to fortify cyber security capabilities across EU member states. In short, the plan would help build a large-scale, comprehensive European cyber defense program. "

20 of the best cyber security podcasts to listen to now

Source: https://www.cybertalk.org/2023/05/04/20-of-the-best-cyber-security-podcasts-to-listen-to-now/

From the Article: "As businesses become increasingly dependent on emerging technology, the importance of strong cyber security has never been more apparent. Stay informed about the latest threats, best practices, tools and perspectives in order to effectively protect your organization from potential cyber attacks."

This New Android FluHorse Malware Steals Passwords & 2FA Codes

Source: https://www.cysecurity.news/2023/05/this-new-android-fluhorse-malware.html

From the Article: "A new Android malware known as 'FluHorse' has been uncovered, which targets users in Eastern Asia with fake applications that seem like legitimate versions. Check Point Research uncovered the malware, which has been targeting various regions of Eastern Asia since May 2022."

Dragon Breath's Latest Double-Clean-App Technique Targeting Gambling Industry

Source: https://www.cysecurity.news/2023/05/dragon-breaths-latest-double-clean-app.html

From the Article: "The Dragon Breath APT group is known for its sophisticated cyber-attacks on a wide range of industries, including the gambling industry. Recently, security researchers have uncovered the group's latest technique: the use of the double-clean-app method to evade detection and infiltrate targeted networks."

Link back to Table of Contents

Imperva Red Team Patches a Privacy Vulnerability in TikTok

Source: https://www.cysecurity.news/2023/05/imperva-red-team-patches-privacy.html

From the Article: "The vulnerability, which has now been patched, was the result of a window message event handler's failure to accurately verify the message's origin, providing attackers access to users' sensitive data."

CERT-In Warns Of 'Royal Ransomware' Virus Attacking India's Critical Sectors

Source: https://www.cysecurity.news/2023/05/cert-in-warns-of-royal-ransomware-virus.html

From the Article: "This malicious malware targets key infrastructure industries, such as manufacturing, communications, healthcare, and education, as well as individuals, encrypting their files and requesting payment in Bitcoin to prevent the release of private information to the public. "

Religious Institutions Become the Latest Focus of Cybercrime Groups

Source: https://www.cysecurity.news/2023/05/religious-institutions-become-latest.html

From the Article: "Over the weekend, two long-standing malicious groups declared their responsibility for attacking religious organizations. This marks a new direction for these groups, as they typically target corporations and government agencies rather than religious institutions."

Vulnerability in Oracle Property Management Software Puts Hotels at Risk

Source: https://www.cysecurity.news/2023/05/vulnerability-in-oracle-property.html

From the Article: "The hundreds of hotels and other hospitality-related organisations across the globe who use Oracle's Opera property management system may wish to immediately patch a bug that Oracle revealed in its April 2023 security update. "

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

Inside the Carrington Mortgage Services Ransomware Attack: Compromised Data and Cybersecurity Measures

Source: https://www.cysecurity.news/2023/05/inside-carrington-mortgage-services.html

From the Article: "Cybersecurity incidents have become increasingly common in the mortgage industry, with multiple lenders and servicers experiencing data breaches that compromised sensitive customer information."

Absolute's 2023 Resilience Index: America's Cybersecurity

Source: https://www.cysecurity.news/2023/05/absolutes-2023-resilience-index.html

From the Article: "Recently, the White House has come up with a new national cybersecurity strategy called 'Absolute's 2023 Resilience Index', it will hold software companies responsible for products' security."

Businesses Must Stay up With Cybercriminals, as They Become More Sophisticated

Source: https://www.cysecurity.news/2023/05/businesses-must-stay-up-with.html

From the Article: "As much as we may want to tune out when we hear about cybersecurity, it is an issue that cannot be ignored. Cybercrime is a constant threat to businesses and individuals alike, and the risks are too great to simply accept and move on."

Hackers Sell Coinbase Accounts for as low as $610 on Dark Web

Source: https://www.cysecurity.news/2023/05/hackers-sell-coinbase-accounts-for-as.html

From the Article: "A recent research by PrivacyAffairs.com notes that hackers target social media logins, credit card numbers, and online banking logins to steal personal information worth $1,010 on the dark web."

Marshals' Computer System Still Down 10 Weeks After Hack

Link back to Table of Contents

Source: https://www.cysecurity.news/2023/05/marshals-computer-system-still-down-10.html

From the Article: "A computer system used by the U.S. Marshals Service to track and hunt fugitives remains down 10 weeks after a hack, raising concerns about the effectiveness of the agency's surveillance efforts."

50 Chinese Hackers for Each FBI Cyber Agent, Bureau Boss Says

Source: https://www.cysecurity.news/2023/05/50-chinese-hackers-for-each-fbi-cyber.html

From the Article: "It is evident from the disclosure that the U.S., in particular, faces several massive cyber threats. There has been a large attack on private and corporate information of the country, more than by any other major nation combined, and it has stolen more data than all of the nations regardless of size."

Data Leak: Critical Data Being Exposed From Salesforce Servers

Source: https://www.cysecurity.news/2023/05/data-leak-critical-data-being-exposed.html

From the Article: "According to a post by KrebsOnSecurity published on Friday, servers running Salesforce software are leaking private data controlled by governmental bodies, financial institutions, and other businesses."

Google Play Blocked 1.43 Million Malicious Apps in 2022

Source: https://www.cysecurity.news/2023/05/google-play-blocked-143-million.html

From the Article: "Google Play store is a very popular app downloader for Android devices because of the heavy presence of people on this store, for reasons alike it has often been targeted by cybercriminals who create malicious apps that are designed to harm users' devices, steal their sensitive credentials and exploit vulnerabilities."

Top 5 Reasons Why Cybersecurity is Essential For Organisations

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

Source: https://www.cysecurity.news/2023/05/top-5-reasons-why-cybersecurity-is.html

From the Article: "After the economies of China and the United States, cybercrime's economy would rank third in size. By 2025, it might grow to $17.65 trillion yearly. We must take action to prevent becoming a victim of cyberattacks given this startling statistic. "

Google Launches Cybersecurity Career Certificate Program

Source: https://www.darkreading.com/careers-and-people/google-now-offers-cybersecurity-career-certificate-program

From the Article: "Google's new program aims to offer accessible training to fill 750K open cybersecurity jobs with diverse array of talent."

Apple Patches Bluetooth Flaw in AirPods, Beats

Source: https://www.darkreading.com/application-security/apple-patches-bluetooth-flaw-in-airpods-beats

From the Article: "Users can check for the updated firmware version of their wireless headphones in the Bluetooth settings of their iPhone, iPad, or Mac devices."

Attackers Route Malware Activity Over Popular CDNs

Source: https://www.darkreading.com/edge-threat-monitor/attackers-route-malware-activity-over-popular-cdns

From the Article: "One way to hide malicious activity is to make it look benign by blending in with regular traffic passing through content delivery networks (CDNs) and cloud service providers, according to a Netskope report."

InsightCyber Launches Platform to Provide Cyber Threat Management and Security to Global Critical Infrastructure

Source: https://www.darkreading.com/application-security/insightcyber-launches-platform-to-provide-cyber-threat-management-and-security-to-global-critical-

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

infrastructure

From the Article: "The InsightCyber Platform delivers continuous AI-monitoring of cyber-physical
assets."

Netskope: Attackers Double Down on Social Engineering Techniques and Malicious Functionalities

Source: https://www.darkreading.com/attacks-breaches/netskope-attackers-double-down-on-social-engineering-techniques-and-malicious-functionalities

From the Article: "Researchers find attackers are successfully evading detection by blending in with normal network traffic via HTTP and HTTPS."

How Public-Private Information Sharing Can Level the Cybersecurity Playing Field

Source: https://www.darkreading.com/threat-intelligence/how-public-private-information-sharing-can-level-the-cybersecurity-playing-field-

From the Article: "Sharing information is critical to help organizations protect data and systems. To be even more effective, collaboration should be inclusive — vendors, researchers, and private companies large and small."

How to Spot a ChatGPT Phishing Website

Source: https://www.darkreading.com/remote-workforce/how-to-spot-a-chatgpt-phishing-website

From the Article: "Scammers are leveraging the popularity of ChatGPT in phishing attacks. Here's a look at research on these newly registered domains and tactics."

Microsoft Digital Defense Report: Key Cybercrime Trends

Source: https://www.darkreading.com/microsoft/microsoft-digital-defense-report-key-cybercrime-trends

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

From the Article: "In part one of this three-part series, Microsoft details how cybercriminals innovate and evade detection to make money or sow destruction."

Microsoft Digital Defense Report: Trends In Device and Infrastructure Attacks

Source: https://www.darkreading.com/microsoft/microsoft-digital-defense-report-trends-in-device-and-infrastructure-attacks

From the Article: "In part two of this three-part series, Microsoft synthesizes the impact of IoT/OT security challenges and offers tips for strengthening security there."

Microsoft Patches Serious Azure Cloud Security Flaws

Source: https://www.darkreading.com/cloud/microsoft-patches-serious-azure-cloud-security-flaws

From the Article: "Three vulnerabilities in the platform's API Management Service could allow access sensitive data, mount further attacks, and even hijack developer portals."

Threat Spotlight: Proportion of Malicious HTML Attachments Doubles Within a Year

Source: https://www.darkreading.com/application-security/threat-spotlight-proportion-of-malicious-html-attachments-doubles-within-a-year

From the Article: "The security industry has been highlighting the cybercriminal misuse of HTML for years — and evidence suggests it remains a successful and popular attack tool. Last year we reported that around one-in-five (21%) of all HTML attachments scanned by Barracuda in May 2022 were malicious."

The Daily Number of Human-Driven Cyber Incidents Increased by 1.5 Times in 2022

Source: https://www.darkreading.com/remote-workforce/the-daily-number-of-human-driven-cyber-incidents-increased-by-1-5-times-in-2022

From the Article: " Research based on the analysis of incidents reported to customers of Kaspersky Managed Detection and Response (MDR) has revealed that Security Operations Center (SOC) analysts discovered more than three high-severity incidents

Link back to Table of Contents

with direct human involvement every day in 2022."

What's the Secret to Finding the Next Big Thing in Cybersecurity?

Source: https://www.darkreading.com/edge-articles/whats-the-secret-to-finding-the-next-big-thing-in-cybersecurity

From the Article: "Varun Badhwar, who has brought each of the three startups he founded to the finals of the RSAC Innovation Sandbox, talks about how to see around the corner."

Anatomy of a Malicious Package Attack

Source: https://www.darkreading.com/vulnerabilities-threats/anatomy-of-a-malicious-package-attack

From the Article: "Malicious packages are hard to avoid and hard to detect — unless you know what to look for."

Legitimate Software Abuse: A Disturbing Trend in Ransomware Attacks

Source: https://www.darkreading.com/application-security/legitimate-software-abuse-a-disturbing-trend-in-ransomware-attacks

From the Article: "Build a culture of security so that everyone is on the lookout for suspect behavior. Implement least privilege, improve visibility."

Meta Expunges Multiple APT, Cybercrime Groups From Facebook, Instagram

Source: https://www.darkreading.com/vulnerabilities-threats/meta-expunges-multiple-apt-cybercrime-groups-from-facebook-instagram

From the Article: "The company has removed three APTs and six potentially criminal networks from its platforms who leveraged elaborate campaigns of fake personas and profiles to lure and compromise users."

Link back to Table of Contents

Hotels at Risk From Bug in Oracle Property Management Software

Source: https://www.darkreading.com/application-security/hotels-at-risk-from-bug-in-oracle-property-management-software

From the Article: "Oracle's characterization of the vulnerability in its Opera software as complex and hard to exploit is incorrect, researchers who found the flaw and reported it say."

Online Pizza Ordering System 1.0 Shell Upload

Source: https://packetstormsecurity.com/files/172182/opos10-shell.txt

From the Article: "Online Pizza Ordering System version 1.0 suffers from an unauthenticated remote shell upload vulnerability."

Fortinet Training Institute Wins Industry Accolades

Source: https://www.fortinet.com/blog/business-and-technology/fortinet-training-institute-industry-accolades

From the Article: "The Fortinet Training Institute has recently been recognized in the industry for its efforts in providing cybersecurity training and certification."

Hackers use WinRAR as a Cyberweapon to Conduct Destructive Cyberattacks

Source: https://gbhackers.com/hackers-winrar-cyberweapon/

From the Article: "CERT-UA (Ukrainian Government Computer Emergency Response Team) recently reported that the Ukrainian state networks suffered a cyber attack attributed to the notorious ‘Sandworm’ hacking group from Russia. The attackers reportedly employed WinRar to destroy critical data on various government devices."

New BGP Protocol Flaws Let Attackers Trigger DoS Attacks

Source: https://gbhackers.com/new-bgp-protocol-flaws/

Link back to Table of Contents
The articles have been 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: "Forescout Vedere Labs recently highlighted the neglected BGP security aspect – software implementation vulnerabilities. FRRouting's BGP message parsing vulnerabilities discovered by Forescout Vedere Labs could enable attackers to trigger a DoS state on susceptible BGP peers."

Malware Campaigns Abusing Telegram Bots to Spread Rapidly

Source: https://gbhackers.com/malware-telegram-bots/

From the Article: "Numerous updates and alterations were witnessed in the major malware families employed in phishing scams during the first quarter of 2023, alongside significant variations in TTPs. "

WordPress plugin vulnerability puts two million websites at risk

Source: https://grahamcluley.com/wordpress-plugin-vulnerability-puts-two-million-websites-at-risk/

From the Article: "Millions of WordPress-powered websites are using the Advanced Custom Fields and Advanced Custom Fields Pro plugins, which security researchers say have been vulnerable to cross-site scripting (XSS) attacks."

Patch now! The Mirai IoT botnet is exploiting TP-Link routers

Source: https://www.tripwire.com/state-of-security/patch-now-mirai-iot-botnet-exploiting-tp-link-routers

From the Article: "Businesses should patch their TP-Link routers as soon as possible, after the revelation that a legendary IoT botnet is targeting them for recruitment."

Cyberpress Launches Cybersecurity Press Release Distribution Platform

Source: https://www.hackread.com/cyberpress-launches-cybersecurity-press-release-distribution-platform-2/

From the Article: "Cybersecurity gets a new dedicated newswire. Cyberpress, a press release distribution platform for the cybersecurity industry, has opened its doors today.

Link back to Table of Contents

This newswire service provides an effective communications approach for cybersecurity companies, public relations agencies and marketing advisors, investment firms operating in the space and more."

Seized: 9 Crypto Laundering Sites Used by Ransomware Gangs

Source: https://www.hackread.com/9-cryptocurrency-laundering-sites-seized/

From the Article: "International cooperation between the Ukrainian Cyber and National Police, the FBI, and the Department of Justice has led to the seizure of cybercriminals' cryptocurrency laundering websites."

The Double-Edged Sword of Crypto in Ransomware

Source: https://www.bankinfosecurity.com/double-edged-sword-crypto-in-ransomware-a-21999

From the Article: "Ransomware hackers' favorite currency is cryptocurrency. Digital assets transfer millions of dollars each year from victims to cybercriminals. But that dependency is also an opportunity for law enforcement to hit ransomware hackers in their most vulnerable spot."

Meta Cracks Down on South Asian Cyberespionage Groups

Source: https://www.bankinfosecurity.com/meta-cracks-down-on-south-asian-cyberespionage-groups-a-21992

From the Article: "Social media giant Meta took down hundreds of fake Facebook and Instagram accounts used by South Asia advanced persistent threat groups to glean sensitive information and coax users into installing malware."

Fortra GoAnyWhere-Related Health Data Breach Tally Climbs

Source: https://www.bankinfosecurity.com/forta-goanywhere-related-health-data-breach-tally-climbs-a-21974

From the Article: "The tally of individuals whose sensitive information was compromised

by the exploitation of a zero-day vulnerability in Fortra's GoAnyWhere secure file transfer software is growing by millions as more entities report heath data breaches to regulators."

WinRAR Weaponized for Attacks on Ukrainian Public Sector

Source: https://www.bankinfosecurity.com/winrar-weaponized-for-attacks-on-ukrainian-public-sector-a-21965

From the Article: "Ukrainian cyber defenders say they spotted a malicious script used to activate the delete option on a Windows file archiving utility likely planted by the Russian intelligence agency unit Sandworm. CERT-UA says attackers likely used a compromised VPN credential to gain access."

Why Gaining Visibility Into Cyberthreats Is a Big Challenge

Source: https://www.bankinfosecurity.com/gaining-visibility-into-organizations-digital-assets-a-21956

From the Article: "A top challenge businesses face is the lack of knowledge about what digital assets they have, making it difficult to protect them, respond to attacks, and collect evidence. External threat intelligence and attack surface management are colliding as companies look to respond effectively to threats."

RTM Locker RaaS Group Turns to Linux, NAS and ESXi Hosts

Source: https://www.bankinfosecurity.com/rtm-locker-raas-group-turns-to-linux-nas-esxi-hosts-a-21909

From the Article: "RTM Locker ransomware-as-a-service operators have now turned their attention to Linux, network-attached storage devices and ESXi hosts. The highly structured group appears to be using a new ransomware strain that shows traces of Babuk ransomware's leaked source code."

Cryptohack Roundup: Merlin, Kucoin, Trust and UniSat Wallet

Link back to Table of Contents

Source: https://www.bankinfosecurity.com/cryptohack-roundup-merlin-kucoin-trust-unisat-wallet-a-21885

From the Article: "Between April 21 and 27, hackers stole $1.8 million from Merlin, $22,638 from Kucoin and $170,000 from Trust Wallet and attacked UniSat Wallet. The U.S. indicted two men for DPRK-linked money laundering, and a U.K. parliamentary panel heard plans to curb cybercrime with better crypto seizure skills."

Breach Roundup: Ukrainian Police Detain a PII Vendor

Source: https://www.bankinfosecurity.com/breach-roundup-ukrainian-police-detain-pii-vendor-a-21883

From the Article: "Every week, Information Security Media Group rounds up cybersecurity incidents and breaches around the world. In the days between April 21 and April 27, the spotlight was on the arrest of a Ukrainian trafficker in stolen data, a U.S. Navy shipbuilder and incidents in Canada, India and Kenya."

SECURITY ALERT: Danish Customers Targeted by Active PostNord DK Phishing Campaign

Source: https://heimdalsecurity.com/blog/security-alert-danish-customers-targeted-by-active-postnord-dk-phishing-campaign/

From the Article: "Heimdal® has recently discovered what can very well be the debut of a massive phishing campaign unfolding in the Nordics. According to a tip sent to us by an anonymous reader, the APT's choice in phishing is an email in which the victim is informed about the status of an unclaimed postal package. "

Week in review: Fake ChatGPT desktop client steals data, Patch Tuesday forecast

Source: https://www.helpnetsecurity.com/2023/05/07/week-in-review-fake-chatgpt-desktop-client-steals-data-patch-tuesday-forecast/

From the Article: "Here's an overview of some of last week's most interesting news, articles, interviews and videos: Former Uber CSO avoids prison for concealing data breach Joe Sullivan, the former Uber CSO who has been convicted last year for attempting to cover up a data breach Uber suffered in 2016 and kept it hidden from the Federal Trade Commission (FTC), has been sentenced to three years of probation plus

200 hours of community service."

Arthur Shield tackles safety and performance issues in large language models

Source: https://www.helpnetsecurity.com/2023/05/04/arthur-shield-firewall/

From the Article: "Arthur introduced a powerful addition to its suite of AI monitoring tools: Arthur Shield, a firewall for large language models (LLMs). This patented new technology enables companies to deploy LLM applications like ChatGPT more safely within an organization, helping to identify and resolve issues before they become costly business problems — or worse, result in harm to their customers."

ChatGPT and other AI-themed lures used to deliver malicious software

Source: https://www.helpnetsecurity.com/2023/05/04/malicious-chatgpt/

From the Article: "Since the beginning of 2023 until the end of April, out of 13,296 new domains created related to ChatGPT or OpenAI, 1 out of every 25 new domains were either malicious or potentially malicious," Check Point researchers have shared on Tuesday."

Apricorn introduces Aegis NVX hardware-encrypted USB storage device

Source: https://www.helpnetsecurity.com/2023/05/04/apricorn-usb-10gbps-aegis-nvx/

From the Article: "Employing proprietary architecture, the Aegis NVX is the first Apricorn encrypted device to feature an NVME SSD inside, to address the immediate protection of raw data delivered directly from its source at high speeds."

Intruder launches continuous attack surface monitoring for SMBs

Source: https://www.helpnetsecurity.com/2023/05/04/intruder-attack-surface-monitoring-capabilities/

From the Article: "Intruder has launched its continuous attack surface monitoring capabilities. The company's new premium plan offering takes vulnerability management to the next level with continuous coverage, increasing visibility and transparency of

external attack surfaces."

How AI is reshaping the cybersecurity landscape

Source: https://www.helpnetsecurity.com/2023/05/04/ai-cybersecurity-landscape-video/

From the Article: "The success of ChatGPT, a text-generation chatbot, has sparked widespread interest in generative AI among millions of people worldwide. According to Jumio's research, 67% of consumers globally are aware of generative AI technologies, and in certain markets, such as Singapore, 45% have utilized an application that employs such technologies"

Amazon Inspector allows search of its vulnerability intelligence database

Source: https://www.helpnetsecurity.com/2023/05/04/amazon-inspector-vulnerability-intelligence-database/

From the Article: "Amazon Inspector is designed to manage vulnerabilities by continuously scanning your AWS workloads for software vulnerabilities and unintended network exposure across your entire organization. "

Top API vulnerabilities organizations can't afford to ignore

Source: https://www.helpnetsecurity.com/2023/05/04/insecure-apis-in-organizations/

From the Article: "75% of organizations typically change or update their APIs on a daily or weekly basis, creating a significant challenge for protecting the changing API attack surface, according to Data Theorem and ESG."

Keysight launches cybersecurity partnership program for MSSPs

Source: https://www.helpnetsecurity.com/2023/05/03/keysight-cybersecurity-partnership-program-mssps/

From the Article: "Keysight Technologies has launched a new cybersecurity partnership program for managed security service providers (MSSP) to improve the security posture of organizations using the breach and attack simulation (BAS) capabilities of Keysight

Threat Simulator."

Avetta releases Cyber Risk Solution for complete supply chain cyber health visibility

Source: https://www.helpnetsecurity.com/2023/05/03/avetta-cyber-risk-solution/

From the Article: "Avetta has released the Cyber Risk Solution, providing a quantitative score that evaluates cyber health in 10 areas and delivers an aggregate grade for each supplier. The Avetta One feature offers a diagnostic cyber health check that identifies potential risk areas for companies to investigate further."

Russian national charged for role in stolen credit card verification scheme

Source: https://cyberscoop.com/russian-charged-try2check-credit-card/

From the Article: "Federal prosecutors in New York unsealed a four-count indictment on Wednesday charging a Russian national with running a service to check the status of stolen credit cards, a scheme that helped facilitate tens of millions of fraudulent credit card checks every year, prosecutors said."

When it comes to online scams, 'ChatGPT is the new crypto'

Source: https://cyberscoop.com/chatgpt-scam-facebook-meta-hackers-malware/

From the Article: "Digital fraudsters are as enamored with ChatGPT as everyone else on the internet and have taken advantage its allure to spread a new strain of malware across Facebook, Instagram and WhatsApp in recent months."

ChatGPT hacking, it's only just begun…

Source: https://www.cybertalk.org/2023/05/03/chatgpt-hacking-its-only-just-begun/

From the Article: "Since its November debut on the world stage, the popular AI-powered chatbot, ChatGPT, has continuously attracted cyber criminal attention. Although OpenAI, has developed security measures to prevent product misuse, these measures have not curtailed hacker pursuits."

Link back to Table of Contents

Global Ransomware Attack Targets VMware ESXi Servers

Source: https://www.cysecurity.news/2023/05/global-ransomware-attack-targets-vmware.html

From the Article: "Cybersecurity firms around the world have recently warned of an increase in cyberattacks, particularly those targeting corporate banking clients and computer servers. The Italian National Cybersecurity Agency (ACN) recently reported a global ransomware hacking campaign that targeted VMware ESXi servers, urging organisations to take action to protect their systems."

US Government Takes Down Try2Check Services Used by Dark Web Markets

Source: https://www.cysecurity.news/2023/05/us-government-takes-down-try2check.html

From the Article: "The US Government, on Wednesday, announced that it had taken down the credit card checking tool 'Try2Check' that apparently gave cybercrime actors access to bulk purchases and sale of stolen credit card credentials to check which cards were legitimate and active."

Online Predators Target Children's Webcams, Study Finds

Source: https://www.cysecurity.news/2023/05/online-predators-target-childrens.html

From the Article: "The Internet Watch Foundation has reported a significant rise in the production of sexual abuse images using webcams and similar recording equipment across the globe. The increase has been staggering, with the number of such images having multiplied ten times since 2019. "

Mobile Menace: McAfee's 2023 Report on the Top Mobile Threats

Source: https://www.cysecurity.news/2023/05/mobile-menace-mcafees-2023-report-on.html

From the Article: "Mobile devices are an essential part of our lives today. From staying connected with our loved ones to handling our finances and work-related tasks,

Link back to Table of Contents

smartphones have become indispensable. However, this convenience comes with a price. "

Healthcare Institutions at Risk Due to Reliance on Technology

Source: https://www.cysecurity.news/2023/05/healthcare-institutions-at-risk-due-to.html

From the Article: "As the healthcare system has become more technology-driven, there has been a significant increase in the use of cloud-based and internet applications for delivering facilities."

2 Years After Colonial Pipeline, US Critical Infrastructure Still Not Ready for Ransomware

Source: https://www.darkreading.com/ics-ot/2-years-after-colonial-pipeline-attack-us-critical-infrastructure-remains-as-vulnerable-to-ransomware

From the Article: "Sweeping changes implemented since the May 2021 cyberattack are helping — but more work remains to be done, security experts say."

New Weaponized Android Apps With 1M Installs Steals 2FA Codes & Passwords

Source: https://gbhackers.com/android-malware-steals-2fa-codes/

From the Article: "Check Point Research has recently published a study revealing the discovery of a previously unknown malware variant dubbed FluHorse. The malware comprises multiple malicious Android apps that impersonate legitimate ones, and unfortunately, most of these fake apps have already been installed by over 1,000,000 users."

Apple and Google join forces to combat AirTag stalking

Source: https://www.bitdefender.com/blog/hotforsecurity/apple-and-google-join-forces-to-combat-airtag-stalking/

From the Article: "Apple and Google have announced that they are teaming up in order to combat the safety risks associated with AirTags and other tracking devices."

Link back to Table of Contents

Cyberpress Launches Cybersecurity Press Release Distribution Platform

Source: https://www.hackread.com/cyberpress-launches-cybersecurity-press-release-distribution-platform-3/

From the Article: "According to Nolen, “Our goal is to provide a reliable and efficient platform that helps businesses improve their marketing and communications strategy. We believe that by providing a more targeted distribution approach, we can help companies reach their target audience and get their message across more effectively.”"

ISMG Editors: Special Focus on Cybersecurity in Government

Source: https://www.bankinfosecurity.com/ismg-editors-special-focus-on-cybersecurity-in-government-a-21997

From the Article: "In the latest weekly update, Venable's Grant Schneider joins ISMG editors to discuss takeaways from the RSA Conference 2023, the state of software supply chain security post-SolarWinds, safeguards to prevent unintended adverse impacts of AI, and whether AI could be used to write and digest SBOMs."

Immersive Labs Resilience Score strengthens executive decision making in cyber crises

Source: https://www.helpnetsecurity.com/2023/05/03/immersive-labs-resilience-score/

From the Article: "Immersive Labs announced the launch of the Immersive Labs Resilience Score. The score measures an organization’s workforce preparedness for cyber attacks and breaches based on Immersive Labs’ years of benchmarking data across industry verticals."

Google Chrome will lose the “lock” icon for HTTPS-secured sites

Source: https://www.helpnetsecurity.com/2023/05/03/google-chrome-https/

From the Article: "In September 2023, Google Chrome will stop showing the lock icon when a site loads over HTTPS, partly due to the now ubiquitous use of the protocol."

Link back to Table of Contents

Tython: Open-source Security as Code framework and SDK

Source: https://www.helpnetsecurity.com/2023/05/03/tython-open-source-security-as-code-framework-sdk/

From the Article: "Development teams utilize automation through Infrastructure as Code (IaC) to facilitate rapid and frequent changes to their cloud-native architectures. Security teams must adopt automation and incorporate security measures into code to keep up with the quickly evolving software development. "

Malicious content lurks all over the web

Source: https://www.helpnetsecurity.com/2023/05/03/malware-downloads-q1-2023/

From the Article: "Attackers are finding new ways to evade detection and blend in with normal network traffic using HTTP and HTTPS to deliver malware, according to Netskope."

Veza for SaaS Apps secures sensitive data against breaches, ransomware, and insider threats

Source: https://www.helpnetsecurity.com/2023/05/03/veza-saas-apps/

From the Article: "Veza has unveiled Veza for SaaS Apps, a solution to deliver access security and governance across SaaS applications, including Salesforce, JIRA, Coupa, Netsuite, GitHub, Gitlab, Slack, and Bitbucket."

ThreatX strengthens API and application protection with Botnet Console and API Catalog 2.0

Source: https://www.helpnetsecurity.com/2023/04/27/threatx-botnet-console-api-catalog-2-0/

From the Article: "ThreatX announced the expansion of its platform offering with the release of a new Botnet Console and API catalog 2.0. These new dashboards, unveiled at RSA Conference 2023, will help security teams rapidly investigate automated threats and attempts to abuse APIs with enhanced metrics, analytics, and visualizations."

Link back to Table of Contents

Generative AI and security: Balancing performance and risk

Source: https://www.helpnetsecurity.com/2023/04/27/generative-ai-security/

From the Article: "Are we moving too fast with AI? This is a central question both inside and outside the tech industry, given the recent tsunami of attention paid to ChatGPT and other generative AI tools."

Tessian Respond enables security teams to identify and respond to email threats

Source: https://www.helpnetsecurity.com/2023/04/27/tessian-respond/

From the Article: "Tessian launched Tessian Respond, a major improvement in how security teams identify and respond to email threats compared to traditional secure email gateway solutions. "

CISOs struggle to manage risk due to DevSecOps inefficiencies

Source: https://www.helpnetsecurity.com/2023/04/27/devsecops-adoption-overcoming-resource-challenges/

From the Article: "As their hybrid and multicloud environments become more complex, and teams continue to rely on manual processes that make it easier for vulnerabilities to slip into production environments, CISOs find it increasingly difficult to keep their software secure, according to Dynatrace."

Corporate boards pressure CISOs to step up risk mitigation efforts

Source: https://www.helpnetsecurity.com/2023/04/26/effective-it-risk-management/

From the Article: "While those working in InfoSec and GRC have high levels of confidence in their cyber/IT risk management systems, persistent problems may be making them less effective than perceived, according to RiskOptics."

Seclore puts risk into focus with new data classification and risk insights capabilities

Source: https://www.helpnetsecurity.com/2023/04/26/seclore-digital-asset-classification-

Link back to Table of Contents

and-risk-insights/

From the Article: "Seclore has released new Digital Asset Classification and Risk Insights capabilities delivering security risk visibility and insights for the most sensitive digital assets within the enterprise, such as intellectual property, and customer and employee personally identifiable information."

An overview of the OSI model and its security threats

Source: https://www.tripwire.com/state-of-security/overview-osi-model-and-its-security-threats

From the Article: "The Open Systems Interconnection (OSI) model is a conceptual framework developed by the International Standards Organization (ISO). It has been in use for over 40 years, and is cited in every computer network book. It is also a favorite resource for just about every cybersecurity exam."

Cybersecurity – Change is coming and that's a good thing

Source: https://www.tripwire.com/state-of-security/cybersecurity-change-coming-and-thats-good-thing

From the Article: "“The cyber economy is the economy” Those words were spoken by the US National Security Advisor way back in 2005, and it is remarkable to see how prescient they were. The economy is not only supported by the cyber world, but that world is entirely data driven. "

Cybersecurity in the Cloud: The Challenging Hurdles It Has To Overcome

Source: https://www.tripwire.com/state-of-security/cybersecurity-cloud-challenging-hurdles-it-has-overcome

From the Article: "Cloud Security Challenges Organizations embracing cloud environments must understand that cloud applications and services have become popular targets for cybercriminals. "

4 Lessons from Fortra's Attack Surface Management Guide

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

Source: https://www.tripwire.com/state-of-security/lessons-fortras-attack-surface-management-guide

From the Article: "Think of all the different points within your organization that provide access to information. That could be your website, the mobile version of your application, your Slack instance, and so much more."

Imperva Red Team Discovers Vulnerability in TikTok That Can Reveal User Activity and Information

Source: https://www.imperva.com/blog/imperva-red-team-discovers-vulnerability-in-tiktok-that-can-reveal-user-activity-and-information/

From the Article: "The Imperva Red Team discovered a vulnerability in TikTok, a popular social media platform with more than one billion users worldwide, that could allow attackers to monitor users' activity on both mobile and desktop devices."

With Imperva's DRA and ServiceNow, you can avoid burning out your cyber security employees

Source: https://www.imperva.com/blog/with-impervas-dra-and-servicenow-you-can-avoid-burning-out-your-cyber-security-employees/

From the Article: "In today's world, CIOs and CISOs are facing a tough reality when it comes to the security staff shortage situation. With the deflating economy, nationalism, cybercrime, and nation-led adversaries, the demand for security personnel has increased, making it challenging for organizations to find and retain skilled security staff."

Critical infrastructure continues to call for more attention two years after Colonial Pipeline ransomware attack

Source: https://industrialcyber.co/critical-infrastructure/critical-infrastructure-continues-to-call-for-more-attention-two-years-after-colonial-pipeline-ransomware-attack/

From the Article: "Two years ago, ransomware hackers struck Colonial Pipeline systems, forcing one of the United States' most important fuel pipeline companies to go offline, resulting in an operational disruption in an abundance of caution to contain the DarkSide ransomware attack."

Link back to Table of Contents

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

FERC publishes final rule, provides incentives for advanced cybersecurity investment

Source: https://industrialcyber.co/utilities-energy-power-water-waste/ferc-publishes-final-rule-provides-incentives-for-advanced-cybersecurity-investment/

From the Article: "The Federal Energy Regulatory Commission (FERC) published a final rule revising its regulations to provide incentive-based rate treatment for the transmission of electric energy in interstate commerce and the sale of electric energy at wholesale in interstate commerce by utilities."

DoD puts forward revision to eligibility criteria of its DIB cybersecurity program, asks for public feedback

Source: https://industrialcyber.co/regulation-standards-and-compliance/dod-puts-forward-revision-to-eligibility-criteria-of-its-dib-cybersecurity-program-asks-for-public-feedback/

From the Article: "The U.S. Department of Defense (DoD) is proposing revisions to the eligibility criteria for the voluntary defense industrial base (DIB) Cybersecurity (CS) program. These revisions will allow a broader community of defense contractors to benefit from bilateral information sharing as when this proposed rule is finalized all defense contractors who are subject to mandatory cyber incident reporting will be able to participate. DoD is also proposing changes to definitions and some technical corrections for readability."

OTORIO secures US patent, claims proprietary algorithm will set standard in OT cybersecurity risk management

Source: https://industrialcyber.co/vendor/otorio-secures-us-patent-uses-proprietary-algorithm-to-set-standard-in-ot-cybersecurity-risk-management/

From the Article: "Industrial cybersecurity vendor OTORIO has secured a patent from the U.S. Patent and Trademark Office (USPTO) for the company’s risk management model and attack graph analysis algorithm. The vendor claims the approach sets a new standard in OT (operational technology) cybersecurity risk management."

Link back to Table of Contents

Microsoft detects Iran turning to cyber-enabled influence operations for greater effect

Source: https://industrialcyber.co/ransomware/microsoft-detects-iran-turning-to-cyber-enabled-influence-operations-for-greater-effect/

From the Article: "Microsoft identified that Iran continues to be a significant threat actor, supplementing its traditional cyberattacks with a new playbook, while leveraging cyber-enabled influence operations (IO) to achieve its geopolitical aims."

Constellation Struck By Ransomware Attack, ALPHV Lays Claim

Source: https://informationsecuritybuzz.com/constellation-struck-ransomware-attack-alphv-lays-claim/

From the Article: "On Thursday, Canadian software firm Constellation Software reported that threat actors had broken into some of its networks and stolen personal information and corporate data."

Meta Unravels Social Media Cyber Espionage Operations In South Asia

Source: https://informationsecuritybuzz.com/meta-unravels-social-media-cyber-espionage-operations-south-asia/

From the Article: "Hundreds of well-developed fake profiles on Facebook and Instagram were used by three separate threat actors to launch separate assaults on users in Southern Asia."

Level Finance Crypto Exchange Hacked, After Two Security Audits

Source: https://informationsecuritybuzz.com/level-finance-crypto-exchange-hacked-after-two-security-audits/

From the Article: "Over $1 million worth of digital assets were stolen from Level Finance, one of the leading cryptocurrency exchanges in the world. The incident happened on April 29, 2023, despite the exchange having gone through two security assessments and audits in the past. "

Link back to Table of Contents

"Kekw" Malware in Python Packages Could Steal Data and Hijack Crypto

Source: https://www.infosecurity-magazine.com/news/kekw-malware-python-packages/

From the Article: "Cyble said the Python security team has now removed the malicious package from PyPI."

Cyber Patrols Lead to Seizure of Stolen Artefacts

Source: https://www.infosecurity-magazine.com/news/cyber-patrols-lead-seizure-stolen/

From the Article: "Items dating back thousands of years recovered in new crackdown."

Brightline Hack Exposes Data of Over 780,000 Child Mental Health Patients

Source: https://www.infosecurity-magazine.com/news/brightline-hack-exposes-data/

From the Article: "Brightline said the breach was due to a zero-day flaw in Fortra GoAnywhere MFT."

Malicious HTML Attachment Volumes Surge

Source: https://www.infosecurity-magazine.com/news/malicious-html-attachment-volumes/

From the Article: "File type remains the most dangerous in email-borne threats."

Android Spyware BouldSpy Linked to Iranian Government

Source: https://www.infosecurity-magazine.com/news/android-spyware-bouldspy-linked/

From the Article: "The mobile malware has been used by threat actors to target minority groups."

Earth Longzhi Uses "Stack Rumbling" to Disable Security Software

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

Source: https://www.infosecurity-magazine.com/news/earth-longzhi-disable-security/

From the Article: "Trend Micro analyzed two separate Earth Longzhi campaigns between 2020 and 2022."

Three-Quarters of Firms Predict Breach in Coming Year

Source: https://www.infosecurity-magazine.com/news/threequarters-firms-predict-breach/

From the Article: "Preparedness is improving, but not by enough."

(ISC)2 Urges Countries to Strengthen Collaboration on Cybersecurity Regulation

Source: https://www.infosecurity-magazine.com/news/isc2-strengthen-collaboration/

From the Article: "A new report examines global approaches to cyber legislation across six jurisdictions."

#RSAC: Google Cloud Introduces Generative AI to Security Tools as LLMs Reach Critical Mass

Source: https://www.infosecurity-magazine.com/news/google-cloud-generative-ai-llms/

From the Article: "Google adds its security large language model to a number of its solutions at the RSA Conference 2023."

Falling Dwell Time May Be Due to Faster Threat Activity

Source: https://www.infosecurity-magazine.com/news/falling-dwell-time-faster-threat/

From the Article: "Sophos warns against simple interpretation of the data."

Capita: Data Was Taken in March Cyber Incident

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

Link back to Table of Contents

The articles have been 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 outsourcer claims customer, employee and supplier info may be at risk."

#CYBERUK23: UK Strengthens Cybersecurity Audits for Government Agencies

Source: https://www.infosecurity-magazine.com/news/k-strengthens-cybersecurity-audits/

From the Article: "GovAssure will mandate all UK government departments to go through annual independent, more robust security audits."

Montana Becomes First US State to Pass TikTok Ban

Source: https://www.infosecurity-magazine.com/news/montana-first-us-state-pass-tiktok/

From the Article: "The ban needs to be signed into law by Republican Governor Greg Gianforte."

European Data at Risk With Tick-box GDPR Compliance and High Cyberattack Volumes

Source: https://www.itsecurityguru.org/2023/05/03/european-data-at-risk-with-tick-box-gdpr-compliance-and-high-cyberattack-volumes/

From the Article: "Yesterday, comforte AG released the findings of a survey conducted on over 500 IT Security Specialists and Chief Information Officers across the UK, France and Germany. The research revealed that European IT and security leaders may be dangerously over-confident in their ability to avoid cyberattacks and mitigate the risk of serious data compromise."

Häfele Recovers from Ransomware Attack using SASE

Source: https://www.itsecurityguru.org/2023/05/03/hafele-recovers-from-ransomware-attack-using-sase/

From the Article: "Following a well-publicised ransomware attack in February 2023,

Link back to Table of Contents

Häfele was able to recover in record time by moving to Cato SASE Cloud. The international manufacturer and supplier of furniture fittings, architectural hardware and lighting products rebuilt its 50+ country, 180-site network in under 30 days."

WordPress plugin "LIQUID SPEECH BALLOON" vulnerable to cross-site request forgery

Source: https://jvn.jp/en/jp/JVN99657911/

From the Article: "WordPress plugin "LIQUID SPEECH BALLOON" contains a cross-site request forgery vulnerability."

[Eye Opener] HTML Phishing Attacks Surge by 100% in 12 Months

Source: https://blog.knowbe4.com/eye-opener-html-phishing-attacks-surge-by-100-in-12-months

From the Article: "The Cyberwire reported: "Barracuda released a study this morning indicating that HTML attacks have doubled since last year."

Ransomware Attacks Surge 91% in a Single Month to Reach an All-Time High

Source: https://blog.knowbe4.com/ransomware-attacks-surge

From the Article: "March saw a huge jump in ransomware compared to January and February, signifying that organizations should expect to see a lot more of these attacks this year."

CNBC: Why Nearly 80% of Leaders are Increasing Cybersecurity Spend

Source: https://blog.knowbe4.com/cnbc-nearly-80-leaders-increasing-cybersecurity-spend

From the Article: "According to a recent EY survey, nearly 80% of business leaders are increasing their cybersecurity investment in the next six to 12 months."

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

Response-Based Business Email Compromise Contributes to 97% of Attacks

Source: https://blog.knowbe4.com/response-based-business-email-compromise

From the Article: "The malwareless and seemingly benign nature of business email compromise emails, mixed with impersonation techniques, are difficult to spot as being malicious, making them even more dangerous."

Walmart Jumps to Top of the List of the Worlds Most Impersonated Brands Used in Phishing Attacks

Source: https://blog.knowbe4.com/worlds-most-impersonated-brands-phishing

From the Article: "Walmart's rise to become the brand most likely to be impersonated in Q1 of this year is a real problem."

Malware Downloads Facilitated by Social Engineering

Source: https://blog.knowbe4.com/malware-by-social-engineering

From the Article: "The most common route for malware infections remains social engineering in its various forms: phishing, vishing, etc. Such approaches take advantage of users' deliberately cultivated willingness to trust communications they receive and to follow the instructions and links such malicious communications carry."

Promising Jobs at the U.S. Postal Service, 'US Job Services' Leaks Customer Data

Source: https://krebsonsecurity.com/2023/05/promising-jobs-at-the-u-s-postal-service-us-job-services-leaks-customer-data/

From the Article: "A sprawling online company based in Georgia that has made tens of millions of dollars purporting to sell access to jobs at the United States Postal Service (USPS) has exposed its internal IT operations and database of nearly 900,000 customers."

CyberSec Community Rolls Out ETHOS – An Open Early Warning System

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

Source: https://latesthackingnews.com/2023/04/29/cybersec-community-rolls-out-ethos-an-open-early-warning-system/

From the Article: "Specifically, ETHOS (Emerging THreat Open Sharing) is an open-source platform sharing threat intel from different cybersecurity leaders. The key firms that joined hands to develop ETHOS include 1898 & Co., ABS Group, Dragos, Nozomi Networks, Claroty, NetRise, Forescout, Network Perception, Tenable, Schneider Electric, and Waterfall Security. Moreover, CISA has also expressed interest in joining the project as required."

Facebook Cracks Down On Malware Actors Targeting Biz Accounts

Source: https://www.scmagazine.com/news/business-continuity/facebook-malware-business-accounts

From the Article: "Meta is warning of the emergence of “aggressive and persistent” new strains of malware targeting business users of popular platforms including Facebook, Gmail and Outlook."

Mirai Botnet Loves Exploiting Your Unpatched TP-Link Routers

Source: https://www.theregister.com/2023/05/02/cisa_exploited_flaws_oracle_apache/

From the Article: "The US government's Cybersecurity and Infrastructure Security Agency (CISA) is adding three more flaws to its list of known-exploited vulnerabilities, including one involving TP-Link routers that is being targeted by the operators of the notorious Mirai botnet."

Oracle WebLogic Server vulnerability added to CISA list as “known to be exploited”

Source: https://www.malwarebytes.com/blog/news/2023/05/oracle-weblogic-server-vulnerability-added-to-cisa-list-as-known-to-be-exploited

From the Article: "This means that Federal Civilian Executive Branch (FCEB) agencies are obliged to remediate the vulnerabilities by May 22, 2023. For the rest of us it means "pay attention," everyone else with a vulnerable entity should do this as fast as possible too."

Link back to Table of Contents

Deconstructing Amadey's Latest Multi-Stage Attack and Malware Distribution

Source: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/deconstructing-amadeys-latest-multi-stage-attack-and-malware-distribution/

From the Article: "McAfee Labs have identified an increase in Wextract.exe samples, that drop a malware payload at multiple stages. "

PHP Packagist supply chain poisoned by hacker "looking for a job"

Source: https://nakedsecurity.sophos.com/2023/05/05/php-packagist-supply-chain-poisoned-by-hacker-looking-for-a-job/

From the Article: "Like PyPI for Pythonistas, Gems for Ruby fans, NPM for JavaScript programmers, or LuaRocks for Luaphiles, Packagist is a repository where community contributors can publish details of PHP packages they've created."

North Korean APT Kimsuky Launches Global Spear-Phishing Campaign

Source: https://www.infosecurity-magazine.com/news/north-korea-kimsuky-spear-phishing/

From the Article: "ReconShark is sent via emails containing OneDrive links leading to documents with malicious macros."

Lawmakers Reintroduce Legislation to Bolster Satellite Cybersecurity

Source: https://www.nextgov.com/cybersecurity/2023/05/lawmakers-reintroduce-legislation-bolster-satellite-cybersecurity/385991/

From the Article: "The bipartisan proposal directs CISA to provide commercial satellite owners and operators with more resources and recommendations to improve their cyber protections."

Capita Admits Some Pension Data Likely Accessed In March Breach

Source: https://www.theregister.com/2023/05/05/capita_pension_data_breach/

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

From the Article: "Capita is telling pension customers that some data contained within its systems was potentially accessed when criminals broke into the outsourcing giant's tech infrastructure earlier this year."

Cisco Warns RCE Bug In EOL IP Phone Adapters Won't Get Patched

Source: https://www.scmagazine.com/news/device-security/cisco-critical-rce-bug-wont-get-patched

From the Article: "Cisco Systems is warning a critical flaw impacting its IP phone ports allow unauthenticated attackers to execute code remotely on targeted devices and gain full admin privileges. It is urging customers still using the impacted model, SPA 112 2-Port Phone Adapters, to upgrade to its Cisco ATA 190 Series Analog Telephone Adapter to mitigate the flaw."

China Labels USA Empire Of Hacking Based On Old Wikileaks Dump

Source: https://www.theregister.com/2023/05/05/china_labels_us_hacking_empire/

From the Article: "The National Computer Virus Emergency Response Center of China and local infosec outfit 360 Total Security have conducted an investigation called "The Matrix" that found the CIA conducts offensive cyber ops, and labelled the United States an "Empire of Hacking"."

Microsoft Warns Iran Increasing Its Cyber Influence Operations

Source: https://www.scmagazine.com/news/threat-intelligence/microsoft-warns-iran-increasing-its-cyber-enabled-influence-operations

From the Article: "Microsoft is warning that Iran is using a new set of preferred techniques that combine its traditional cyberattacks with cyber-enabled influence operations (IO) for greater geopolitical effect."

Russia's APT28 Targets Ukraine With Bogus Windows Updates

Source: https://www.theregister.com/2023/05/02/russia_apt28_ukraine_phishing/

Link back to Table of Contents
The articles have been 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 Kremlin-backed threat group APT28 is flooding Ukrainian government agencies with email messages about bogus Windows updates in the hope of dropping malware that will exfiltrate system data."

Boards Are Having the Wrong Conversations About Cybersecurity

Source: https://hbr.org/2023/05/boards-are-having-the-wrong-conversations-about-cybersecurity

From the Article: "Boards that struggle with their role in providing oversight for cybersecurity create a security problem for their organizations. Even though boards say cybersecurity is a priority, they have a long way to go to help their organizations become resilient to cyberattacks. And by not focusing on resilience, boards fail their companies."

20 Hottest Cybersecurity Products At RSAC 2023

Source: https://www.crn.com/news/security/20-hottest-cybersecurity-products-at-rsac-2023

From the Article: "At the start of RSAC 2023, Proofpoint unveiled new capabilities for its Aegis Threat Protection platform that aim to help with thwarting attacks based on account takeovers. The new capabilities include Supplier Threat Protection, which detects compromised supplier accounts and enables simplified investigation into the issues."

New Cactus ransomware encrypts itself to evade antivirus - Bleeping Computer

Source: https://www.bleepingcomputer.com/news/security/new-cactus-ransomware-encrypts-itself-to-evade-antivirus/

From the Article: "A new ransomware operation called Cactus has been exploiting vulnerabilities in VPN appliances for initial access to networks of “large commercial entities.”"

Payment processing: How to avoid the main PayPal scams - Digital Journal

Link back to Table of Contents
The articles have been 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.digitaljournal.com/life/payment-processing-how-to-avoid-the-main-paypal-scams/article

From the Article: "PayPal scams come in various forms, such as shipping address, overpayment, fake email, phishing, hacked PayPal, and fake accounts. To protect consumers from scams, it is important stay informed and keep checking each stage."

Exploit released for 9.8-severity PaperCut flaw already under attack

Source: https://voonze.com/exploit-released-for-9-8-severity-papercut-flaw-already-under-attack/

From the Article: "Exploit code for a critical printer software vulnerability became publicly available on Monday in a release that may exacerbate the threat of malware attacks that have already been underway for the past five days."

MSI victim of ransomware attack Update: MSI has not paid, also Intel Bootguard keys online ...

Source: https://game-news24.com/2023/05/07/msi-victim-of-ransomware-attack-update-msi-has-not-paid-also-intel-bootguard-keys-online-haven-t-paid-also-tv-keys-to-bootguard/

From the Article: "MSI is dead. Money Message claimed that it held hostage 1.5 TB of source code and databases, and demanded 4 million dollars. The code would include the framework in which MSI bios runs and the key to signing a new bios update."

Trend Micro Blocks Over 15 Million Cyber Threats in Bahrain, According to 2022 Report

Source: https://www.albawaba.com/business/pr/trend-micro-blocks-over-15-million-cyber-threats-bahrain-according-2022-report-1517791

From the Article: "Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global leader in cybersecurity, today announced the findings of its annual cybersecurity report, which revealed a significant 55% increase in global threat detections and a massive 242% surge in blocked malicious files in 2022."

Link back to Table of Contents

Ransomware Attacks Increasingly Using AuKill Malware to Disable EDR – Gridinsoft Blogs

Source: https://gridinsoft.com/blogs/ransomware-attacks-increasingly-using-aukill-malware-to-disable-edr/

From the Article: "A new cybercrime tool called “AuKill” has emerged, which attackers use to disable endpoint detection and response (EDR) defenses used by enterprises before deploying ransomware."

Surging Ransomware Threats and Remedies for CISOs

Source: https://www.bankinfosecurity.com/vishak-raman-rsa-video-a-13900

From the Article: "The ransomware threat is becoming increasingly pervasive. At least 10,000 different variants are victimizing organizations that thought they were well-prepared to tackle this growing menace, said Vishak Raman of Fortinet, which recently released a report on ransomware trends."

The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years

Source: https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years

From the Article: "Today marks two years since a watershed moment in the short but turbulent history of cybersecurity. On May 7, 2021, a ransomware attack on Colonial Pipeline captured headlines around the world with pictures of snaking lines of cars at gas stations across the eastern seaboard and panicked Americans filling bags with fuel, fearful of not being able to get to work or get their kids to school."

Ransomware Protection Software Market 2023 Growth Opportunities and Future Outlook - Fylladey

Source: https://fylladey.com/2023/05/ransomware-protection-software-market-2023-growth-opportunities-and-future-outlook-top-companies-microsoft-sophos-intel-security-symantec-kaspersky-lab-malwarebytes-avast-software-cisco-syst/

From the Article: "The Global Ransomware Protection Software Market research looks

at the marketing techniques, active rising trends, and industry contributions of past and present top firms."

In a new hacking crime wave, more personal data is being held hostage - Vigour Times

Source: https://vigourtimes.com/in-a-new-hacking-crime-wave-more-personal-data-is-being-held-hostage/

From the Article: "Joe McMann, head of cybersecurity services at Binary Defense, a cybersecurity solutions provider, said the new battleground is data extortion and companies need to shift gears to face the threat."

The Column: Public information another victim of city's cyberattack - Lowell Sun

Source: https://www.lowellsun.com/2023/05/07/the-column-public-information-another-victim-of-citys-cyberattack

From the Article: "According to the city's initial statement, "Payments for Real Estate, Personal Property, Motor Vehicle Excise, Water Utility, Vital Records, Burial Permits, Cemetery Lot purchases, and other services are still being accepted through the City's online Invoice Cloud payment system. However, payments may not be immediately reflected against payments due online.""

Colonial Pipeline attack: two year anniversary

Source: https://www.worldpipelines.com/special-reports/07052023/colonial-pipeline-attack-2-year-anniversary/

From the Article: "In the early hours of 7 May 2021, a Colonial Pipeline worker discovered a ransom note inside the company's IT systems. Threat actors linked to the DarkSide ransomware organisation had gained access to an outdated VPN account. What followed was one of the most consequential cyberattacks on US energy infrastructure to date, on the largest refined products pipeline in the country."

49% Increase In Phishing Attacks In Egypt During 1Q 2023: Kaspersky - Dailynewsegypt

Source: https://menafn.com/1106191771/49-Increase-In-Phishing-Attacks-In-Egypt-

During-1Q-2023-Kaspersky-Dailynewsegypt

From the Article: "Hasbini shared some Kaspersky statistics on the most common phishing attacks in the Middle East, Turkey and Africa. The statistics showed an increase of 49% in phishing attacks in Egypt during the first quarter of this year compared to the same period last year."

TUSD personal data exposed on dark web after cyberattack - Arizona Daily Star

Source: https://tucson.com/news/local/education/tusd-personal-data-exposed-on-dark-web-after-cyberattack/article_496e38ea-ead7-11ed-96f9-9b577ed3f36c.html

From the Article: "Cybercriminals made off with confidential data about Tucson Unified School District employees and students and put it on the dark web for public access, Bloomberg News reports."

Western Digital restores My Cloud services after cyber attack - InfotechLead

Source: https://infotechlead.com/security/western-digital-restores-my-cloud-services-after-cyber-attack-78197

From the Article: "The unauthorized party obtained customer names, telephone numbers and partial credit card numbers from its systems, Western Digital said in a statement."

A rough year: first a ransomware attack, then a credential stuffing attack affecting more than 1 million patients.

Source: https://www.databreaches.net/a-rough-year-first-a-ransomware-attack-then-a-credential-stuffing-attack-affecting-more-than-1-million-patients/

From the Article: "NextGen, a business associate to medical professionals, reported that between March 29 and April 14, an unauthorized individual accessed “a limited set of electronically stored personal information.” The type of information involved included name, date of birth, address, and social security number."

India records 18% surge in weekly cyber-attacks in Q1 2023: Report - Bizz Buzz

Link back to Table of Contents
The articles have been 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.bizzbuzz.news/technology/india-records-18-surge-in-weekly-cyber-attacks-in-q1-2023-report-1216518

From the Article: "According to Check Point Research (CPR), the global weekly cyber attacks rose by 7 per cent in Q1 2023 versus the same quarter last year, with each organisation facing an average of 1,248 attacks per week."

How hackers are recruiting on the dark web - The Times

Source: https://www.thetimes.co.uk/article/how-hackers-are-recruiting-on-the-dark-web-mpl2hvsss

From the Article: "On a murky part of the internet known as the dark web lies its vacancy board, translated into broken English. For would-be applicants, it details a job description, code of conduct, salary expectations and even a commitment to diversity that would not look out of place in any reputable FTSE-100 company."

Twitter says 'security incident' exposed private Circle tweets - Bleeping Computer

Source: https://www.bleepingcomputer.com/news/security/twitter-says-security-incident-exposed-private-circle-tweets/

From the Article: "Twitter Circle is a feature released in August 2022 that allows users to send tweets to a small circle of people, promising to keep them private from the public."

Keep files safe from cyber criminals with Koofr Cloud Storage, just $140 for life | Macworld

Source: https://www.macworld.com/article/1807625/keep-files-safe-from-cyber-criminals-with-koofr-cloud-storage-just-140-for-life.html

From the Article: "Subscribers who take advantage of this offer receive lifetime access to 1TB of secure space, which is ample for most people. With it, you can keep your important work documents, financial statements, and even family photos safe for many years to come. And you'll never be asked to renew your subscription or pay any extra fees down the road, so it's about as economical as cloud storage gets."

Link back to Table of Contents

Bluefield University's alert system compromised by AvosLocker ransomware | SC Media

Source: https://www.scmagazine.com/brief/breach/bluefield-universitys-alert-system-compromised-by-avoslocker-ransomware

From the Article: "The reality is no organization is insusceptible to a breach – and security teams, alongside the C-suite, should prepare now to make the response more seamless once a crisis does happen."

NSF funds institute to research AI-cybersecurity | The Manila Times

Source: https://www.manilatimes.net/2023/05/07/business/sunday-business-it/nsf-funds-institute-to-research-ai-cybersecurity/1890234

From the Article: "That's why a group of the nation's best computer scientists and engineers, including researchers from Purdue University, have come together to form the National Science Foundation-sponsored Institute for Agent-based Cyber Threat Intelligence and Operation (Action)."

UAE issues cyberattack warning to public and private sectors - The National

Source: https://www.thenationalnews.com/uae/government/2023/05/06/uae-issues-cyberattack-warning-to-public-and-private-sectors/

From the Article: "The council urged public and private entities to activate the Emirates' emergency response system, which would involve sharing data with authorities to limit the prospect of incidents."

Anti-Ransomware Software Market – Industry Trends and Forecast to 2030 - Fylladey

Source: https://fylladey.com/2023/05/anti-ransomware-software-market-industry-trends-and-forecast-to-2030-key-playerszscaler-comodo-hitmanpro/

From the Article: "The study covers every aspect of the Global Anti-Ransomware Software Market, including growth drivers, current trends, prospects, advancements, and the competitive environment."

Link back to Table of Contents

Be careful what and where you click: How to avoid ransomware scams - Digital Journal

Source: https://www.digitaljournal.com/tech-science/be-careful-what-and-where-you-click-how-to-avoid-ransomware-scams/article

From the Article: "In the U.S., the FBI is attempting to coordinate, in conjunction with the city of Dallas, Texas, a cybersecurity response to a ransomware incident that has disrupted several key public services."

Pastor John Gray's church hit by ransomware attack | U.S. News - Christian Post

Source: https://www.christianpost.com/news/pastor-john-grays-church-hit-by-ransomware-attack.html

From the Article: "Relentless Church in South Carolina has suffered a ransomware attack and its head Pastor John Gray cautioned the culprits, warning, “You’re not attacking us, you’re attacking the God that we serve.”"

'Ransomware cult' claims to have hacked two local schools - Queen City News

Source: https://www.qcnews.com/news/u-s/north-carolina/mecklenburg-county/ransomware-cult-claims-to-have-hacked-two-local-schools/

From the Article: "Folders containing sensitive information were published on Twitter by a group claiming to have hacked into Socrates Academy in Matthews and Movement School."

Towns say preparation invaluable in fight against ransomware | News - IndependentRI.com

Source: https://www.independentri.com/news/article_c321ba66-e9ee-11ed-8969-bb77ac70be33.html

From the Article: "North Kingstown recently faced the threat of one but quickly beat back any effort to extort money for unlocking information that was illegally accessed. Narragansett and South Kingstown officials said their towns have strong protections in place."

Link back to Table of Contents
The articles have been 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 watchers are finding creative ways to track attacks | SC Media

Source: https://www.scmagazine.com/analysis/ransomware/ransomware-watchers-creative-ways-track-attacks

From the Article: "Law enforcement, businesses and other stakeholders know on a general level that the cadence and volume of successful attacks are vast and have gotten considerably worse in the past five years, but due to a lack of standardization and reporting from victims, they've historically struggled to understand the number of victims hit each year, which industries, and whether those numbers are getting better or worse as policymakers implement a coterie of responses in the U.S. and abroad."

Harvard Pilgrim Health Care owner targeted by ransomware cyberattack - WMTW

Source: https://www.wmtw.com/article/harvard-pilgrim-health-care-owner-targeted-ransomware-cyberattack/43807857

From the Article: "The company that owns Harvard Pilgrim Health Care and other major health insurance plans is responding to a ransomware attack. Point32Health released a statement stating that their staff identified a cybersecurity breach on April 17, impacting the systems used to connect to members, accounts, brokers and providers."

South Carolina: Church becomes latest victim of ransomware attack - WYFF

Source: https://www.wyff4.com/article/church-south-carolina-ransomware-attacks-victim/43807002

From the Article: "The list of Upstate entities recently breached by malware or ransomware now has a place of God on it.Relentless Church, a community powerhouse known as a multi-cultural, non-denominational place of worship with thousands of members, was the recent victim of a ransomware attack."

Organizations slow to patch GoAnywhere MFT vulnerability even after Clop ransomware attacks

Source: https://therecord.media/organizations-slow-to-patch-goanywhere-vulnerability-after-clop-attacks

From the Article: "Dozens of organizations are still exposed to cyberattacks through a

widely-abused vulnerability in GoAnywhere MFT — a web-based tool that helps organizations transfer files — according to new research."

CISA Rolls Out Program to Protect Critical Infrastructure From Ransomware

Source: https://www.informationweek.com/security-and-risk-strategy/cisa-rolls-out-new-program-to-protect-critical-infrastructure-from-ransomware-

From the Article: "The Cybersecurity and Infrastructure Security Agency (CISA) has established the Ransomware Vulnerability Warning Pilot (RVWP) in an effort to mitigate ransomware attacks against critical infrastructure entities. This new program, authorized by the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) of 2022, recently sent out an initial round of vulnerability notifications to 93 organizations."

Nonprofit-led ransomware task force reviews progress on key recommendations with two ...

Source: https://insidecybersecurity.com/daily-news/nonprofit-led-ransomware-task-force-reviews-progress-key-recommendations-two-year

From the Article: "The Institute for Security and Technology's Ransomware Task Force is looking back at its progress over the past two years since the release of a foundational report, with an event today and a new status update that describes key milestones achieved and what they plan to work on in the coming months."

ALPHV gang claims ransomware attack on Constellation Software - Bleeping Computer

Source: https://www.bleepingcomputer.com/news/security/alphv-gang-claims-ransomware-attack-on-constellation-software/

From the Article: "Canadian diversified software company Constellation Software confirmed on Thursday that some of its systems were breached by threat actors who also stole personal information and business data."

Ransomware Task Force: Data Sharing Needed to 'Build a Clear Picture' - Duo Security

Source: https://duo.com/decipher/ransomware-task-force-data-sharing-needed-to-build-

a-clear-picture

From the Article: "A critical piece in defending against ransomware is data sharing - however, a new report shows that private sector organizations, governments and cryptocurrency entities still need to make progress in working together to swap information about cyber incidents."

CERT-In warns organisations against Royal Ransomware for targeting critical infrastructure

Source: https://www.moneycontrol.com/europe/?url=https://www.moneycontrol.com/news/business/cert-in-warns-organisations-against-royal-ransomware-for-targeting-critical-infrastructure-10531781.html

From the Article: "The Indian Computer Emergency Response Team (CERT-In) has warned users against ViperSoftX, an information stealing malware and Royal Ransomware that has been targeting multiple critical infrastructure sector, the agency said in recent advisories."

Ransomware actors are actively exploiting a critical Remote Code Execution vulnerability in ... - | Cert

Source: https://www.cert.be/en/warning-ransomware-actors-are-actively-exploiting-critical-remote-code-execution-vulnerability

From the Article: "PaperCut produces printing management software for Canon, Epson, Xerox, and almost every other major printer brand. Its tools are used by more than 70,000 organizations, including government agencies, universities, and large companies around the world."

More Swiss media groups affected by ransomware attack - SWI swissinfo.ch

Source: https://www.swissinfo.ch/eng/business/more-swiss-media-groups-affected-by-ransomware-attack/48488756

From the Article: "At Tamedia, delivery addresses from the same cantons have reportedlyExternal link been published on the dark web. This is a part of the internet hosted within an encrypted network and accessible only through specialised anonymity-

providing tools."

Cyber alert issued against 'Royal' ransomware that attacks health, education sectors, ET CIO

Source: https://cio.economictimes.indiatimes.com/news/digital-security/cyber-alert-issued-against-royal-ransomware-that-attacks-health-education-sectors/100001598

From the Article: "The Indian cyber security agency has issued a warning against the "Royal ransomware" virus that attacks critical sectors like communications, healthcare, education, and even individuals and seeks pay-off in Bitcoins for not leaking personal data in the public domain."

Ransomware group behind Oakland attack targets city in Massachusetts

Source: https://therecord.media/lowell-massachusetts-city-ransomware-attack-play-cybercrime

From the Article: "The cybercrime group that launched a devastating attack on the city of Oakland has taken credit for yet another breach of a local government — this time naming the Massachusetts city of Lowell as its latest victim."

AvidXchange hit by a second major ransomware attack this year - TechRadar

Source: https://www.techradar.com/news/payment-giant-avidxchange-suffers-second-ransomware-attack-of-2023

From the Article: "AvidXchange has suffered its second major ransomware attack of 2023 after hackers published a sample of the stolen data on their website and demanded a ransom be paid as soon as possible. "

What Is Royal Ransomware? CERT-In Warns Organisations Against Attacks Targeting ...

Source: https://www.bqprime.com/technology/bqc-what-is-royal-ransomware-cert-in-warns-organisations-against-attacks-targeting-critical-infrastructure

From the Article: "The Indian Computer Emergency Response Team (CERT-In) recently

issued a warning against “Royal ransomware,” that has been attacking critical sectors such as healthcare, communications, and education since it was first detected in January 2022."

Influential task force takes stock of progress against ransomware - The Washington Post

Source: https://www.washingtonpost.com/politics/2023/05/05/influential-task-force-takes-stock-progress-against-ransomware/

From the Article: "A lot has changed since then. Days after the report’s release, a ransomware attack hit Colonial Pipeline and sparked a fuel panic — an incident that was one of the main triggers for the Biden administration to shift gears on how to approach cybersecurity. Of late, there’s evidence that ransomware has been experiencing if not an active decline, then a lull in its effectiveness in some ways."

Post-CRC Case Study: Prolock Ransomware - Chainalysis Academy

Source: https://academy.chainalysis.com/post-crc-case-study-prolock-ransomware

From the Article: "Learn more about tracing funds, creating custom clusters, and identifying peelchains in this ransomware case study."

Why Educational Institutions are Prone to Ransomware Attacks (and What They Can Do to ...

Source: https://thejournal.com/articles/2023/05/04/why-educational-institutions-are-prone-to-ransomware-attacks.aspx

From the Article: "Ransomware is the most significant cyber threat in the education sector, and K–12 schools and colleges and universities are both targets. We remember the effects on Los Angeles Unified School District, the second-largest district in the U.S. with more than 1,000 schools and 600,000 students, when it was hit by a ransomware attack, disrupting access to its IT systems."

BU cyberattack: cybersecurity experts discuss ransomware - WVVA

Link back to Table of Contents
The articles have been 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.wvva.com/2023/05/05/bu-cyberattack-cybersecurity-experts-discuss-ransomware/

From the Article: "As we reported Monday, hackers targeting Bluefield University are threatening to release the private information of thousands of students onto the dark web unless Bluefield University agrees to pay their ransom of an unknown amount. This leaves Bluefield University with this question: 'to pay or not to pay.'"

Cyber alert issued against 'Royal' ransomware that attacks health, education sectors

Source: https://www.tribuneindia.com/news/nation/cyber-alert-issued-against-royal-ransomware-that-attacks-health-education-sectors-504747

From the Article: "'The ransomware encrypts files on a victim's system and attackers ask for ransom payment in bitcoin," CERT-In says in an advisory."

PowerShell used in 76% of ransomware incidents: Attacks on education sector surge

Source: https://thestack.technology/powershell-use-for-ransomware/

From the Article: "PowerShell was used in 76% of ransomware attacks in April 2023 according to new data from cybersecurity company BlackFog."

Harnessing the G20's Potential for Global Counter-Ransomware Efforts | ORF

Source: https://www.orfonline.org/research/harnessing-the-g20s-potential-for-global-counter-ransomware-efforts/

From the Article: "Since the WannaCry and NotPetya attacks in 2017, ransomware has emerged as a potent cybersecurity threat to states and citizens alike."

Sydney Westmead cancer centre targeted by ransomware attack | news.com.au

Source: https://www.news.com.au/national/crime/hackers-demand-hefty-sum-as-authorities-confirm-sydney-cancer-centre-targeted-in-ransomware-attack/news-story/ebf956ffdf6ba3fede45f4882a2c7ab4

Link back to Table of Contents

From the Article: "A major cancer treatment centre has been targeted by hackers, with the group giving the centre just seven days to fork over $100,000 or risk personal data being released online."

TSMC, partners plan to invest up to $11 billion in German fabrication plant, Bloomberg reports

Source: https://www.reuters.com/markets/deals/tsmc-partners-plan-up-11-bln-investment-german-fabrication-plant-bloomberg-news-2023-05-03/

From the Article: "The venture between TSMC, NXP Semiconductors NV (NXPI.O), Robert Bosch GmbH and Infineon Technologies AG (IFXGn.DE) will have a budget of at least 7 billion euros, including state subsidies, but is likely to end up closer to 10 billion euros, according to the report."

Subscriptions Required

Taiwan's Trade Clash with China Could Benefit the U.S.

Source: https://www.wsj.com/articles/taiwans-trade-clash-with-china-could-benefit-the-u-s-d26ef63d?mod=Searchresults_pos1&page=1

From the Article: "Taiwan is preparing for a sharp rise in economic tensions, including encouraging businesses to look to invest elsewhere"

Biden Secured Trillions in Domestic Spending. Now Comes the Hard Part.

Source: https://www.wsj.com/articles/biden-secured-trillions-in-domestic-spending-now-comes-the-hard-part-a0fbe4d6?mod=Searchresults_pos2&page=1

From the Article: "President is reorienting government to focus on implementation and making sure money is spent efficiently"

WSJ News Exclusive | Ford Hits Production Snag on F-150 Trucks Due to Missing Door Handles

Source: https://www.wsj.com/articles/ford-hits-production-snag-on-f-150-trucks-due-to-missing-door-handles-5e8dbe06?mod=Searchresults_pos3&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: "Auto maker is building trucks with temporary door handles and then parking them until correct ones are available"

On Biden's Second-Term Agenda: Unmet Goals From His First Term

Source: https://www.wsj.com/articles/on-bidens-second-term-agenda-unmet-goals-from-his-first-term-a9ec64de?mod=Searchresults_pos4&page=1

From the Article: "Mr. Biden has signaled that he will push for universal prekindergarten, expanded eldercare benefits and more affordable housing if he earns a second term. The president included these ideas in his roughly $3.5 trillion agenda aimed at strengthening the country's social safety net known as Build Back Better, but Congress whittled that down significantly."

U.S. Trade With World Rose in March on Energy, Auto Shipments

Source: https://www.wsj.com/articles/u-s-trade-with-world-rose-in-march-on-energy-auto-shipments-f7867d09?mod=Searchresults_pos6&page=1

From the Article: "Businesses in the U.S. shipped more goods to China after the world's second-largest economy lifted Covid restrictions"

The Gas-Guzzler Business Is Still Trucking

Source: https://www.wsj.com/articles/the-gas-guzzler-business-is-still-trucking-e7bb71ef?mod=Searchresults_pos8&page=1

From the Article: "While investors worry about Tesla's price war, Detroit's oligopoly in pickup trucks and large sport-utility vehicles continues to churn out profit"

Dow Industrials Inch Lower After Regulators Seize First Republic

Source: https://www.wsj.com/articles/global-stocks-markets-dow-news-05-01-2023-8893eb05?mod=Searchresults_pos9&page=1

From the Article: "Regional bank stocks were among the weakest performers in

Monday’s quiet session"

The Building Boom Is Prolonging Market Pain

Source: https://www.wsj.com/articles/the-building-boom-is-prolonging-market-pain-b224eb74?mod=Searchresults_pos10&page=1

From the Article: "Construction employment is higher than ever—undermining bets the Fed will soon pivot"

Big Tech Expects Some Assets to Last Longer. But the Boost to Profit Is Temporary.

Source: https://www.wsj.com/articles/big-tech-expects-some-assets-to-last-longer-but-the-boost-to-profit-is-temporary-66ce9f98?mod=Searchresults_pos11&page=1

From the Article: "Extension of the working lives of technical equipment allows companies like Alphabet, IBM and Akamai Technologies to improve their efficiency and profitability as they cut costs"

A Debt Deal Could Help Solve the Country’s Inflation Problem

Source: https://www.wsj.com/articles/a-debt-deal-could-help-solve-the-countrys-inflation-problem-bef121c?mod=Searchresults_pos12&page=1

From the Article: "Spending cuts could prompt the Fed to cut interest rates sooner, easing some of the pressure on banks"

Regional Bank Shares Fall, Ahead of Fed’s Expected Rate Hike - What’s News - WSJ Podcasts

Source: https://www.wsj.com/podcasts/whats-news/regional-bank-shares-fall-ahead-of-feds-expected-rate-hike/32f5fb25-af50-4530-a8fb-f4f19306fd9d?mod=Searchresults_pos13&page=1

From the Article: "P.M. Edition for May 2. Shares of regional banks fell sharply on Tuesday. The declines come after First Republic struck a deal to sell the bulk of its operations to JPMorgan Chase and before an expected rate-hike decision from the

Federal Reserve. Plus, WSJ economics reporter Harriet Torry discusses President Biden's record on the economy, as he launches his re-election bid. Annmarie Fertoli hosts."

First Republic Bank Is Seized and Sold to JPMorgan - What's News - WSJ Podcasts

Source: https://www.wsj.com/podcasts/whats-news/first-republic-bank-is-seized-and-sold-to-jpmorgan/aed893fa-4531-46b0-9cc8-4a4cbf92815a?mod=Searchresults_pos14&page=1

From the Article: "A.M. Edition for May 1. U.S. regulators have seized First Republic Bank and struck a deal to sell the bulk of the lender's operations to JPMorgan. The Journal's Quentin Webb breaks down the second-largest bank failure in U.S. history and whether more banking turmoil is to come. Plus, the air comes out of the U.S. Dollar. And President Biden calls for the release of jailed WSJ journalist Evan Gershkovich. Luke Vargas hosts."

Risks to Journalists Grow; Markets on Edge Ahead of Fed Decision - What's News - WSJ Podcasts

Source: https://www.wsj.com/podcasts/whats-news/risks-to-journalists-grow-markets-on-edge-ahead-of-fed-decision/b5d46b95-ef14-408d-aeea-d2e52034cfff?mod=Searchresults_pos15&page=1

From the Article: "A.M. Edition for May 3. A record number of reporters were imprisoned last year, according to the Committee to Protect Journalists. WSJ international editor Grainne McCarthy discusses Russia's detention of WSJ reporter Evan Gershkovich and how newsrooms are coping with eroding press freedom."

Qualcomm Sees No Immediate Smartphone Demand Recovery

Source: https://www.wsj.com/articles/qualcomm-qcom-q2-earnings-report-2023-99c0fd5a?mod=Searchresults_pos2&page=1

From the Article: "Mobile-phone chip maker is diversifying into new areas as its core market slows"

Link back to Table of Contents

Technology and AI are Changing Jobs at Walmart: Here's How - As We Work - WSJ Podcasts

Source: https://www.wsj.com/podcasts/as-we-work/technology-and-ai-are-changing-jobs-at-walmart-heres-how/7705fff7-0f91-4795-8299-260140475348?mod=Searchresults_pos3&page=1

From the Article: "Walmart is one of the world's largest retailers. With 2.1 million workers, it's also one of the world's largest private employers, and it's hiring, including for tech jobs you'd expect to see in Silicon Valley."

As Generative AI Gets Hotter, KKR Bets on Keeping Data Centers Cool

Source: https://www.wsj.com/articles/as-generative-ai-gets-hotter-kkr-bets-on-keeping-data-centers-cool-d3d62cc7?mod=Searchresults_pos11&page=1

From the Article: "Investment firm will acquire CoolIT Systems, maker of systems designed to prevent computing hardware from overheating"

Apple Connects Through Economic Jitters

Source: https://www.wsj.com/articles/apple-connects-through-economic-jitters-6bed3b1f?mod=Searchresults_pos18&page=1

From the Article: "Resilient iPhone sales help an otherwise weak quarter"

Samsung Is a Case Study in How Manufacturers Leave China

Source: https://www.wsj.com/articles/samsung-is-a-case-study-in-how-manufacturers-leave-china-5dcb2dcf?mod=Searchresults_pos1&page=2

From the Article: "Company still has significant operations in China but its smartphone manufacturing business pulled up stakes years ago"

Opinion | In Hollywood Strike, AI Is Nemesis

Source: https://www.wsj.com/articles/in-hollywood-strike-ai-is-nemesis-script-writer-

Link back to Table of Contents
The articles have been 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-algorithm-830179ad?mod=Searchresults_pos2&page=2

From the Article: "If the Netflix algorithm is unable to recommend a show we'll like, maybe it can create one instead."

China's Tightening Grip on Foreign Firms Risks Hitting Investment

Source: https://www.wsj.com/articles/chinas-tightening-grip-on-foreign-firms-risks-hitting-investment-93389517?mod=Searchresults_pos11&page=2

From the Article: "Some gauges suggest overseas inflows to the Chinese economy have stagnated"

U.S. Companies in China Worry Due Diligence Will End in Spy Dramas

Source: https://www.wsj.com/articles/foreign-firms-in-china-squeezed-by-u-s-disclosure-demands-beijings-security-clampdown-658ef8f?mod=Searchresults_pos13&page=2

From the Article: "Firms doing critical on-the-ground vetting are on heightened alert as Chinese authorities ramp up police visits"

Elon Musk Tries to Direct AI—Again

Source: https://www.wsj.com/articles/elon-musk-ai-chatgpt-artificial-intelligence-x-69464a1?mod=Searchresults_pos14&page=2

From the Article: "His latest startup follows a decade of being outmaneuvered in his quest to steer the development of artificial intelligence"

Canada Passes Law Aimed at Exposing Forced Labor in Supply Chains

Source: https://www.wsj.com/articles/canada-passes-law-aimed-at-exposing-forced-labor-in-supply-chains-e13c289?mod=Searchresults_pos2&page=1

From the Article: "The law will require more reporting from companies, but critics say it falls short"

Link back to Table of Contents

The articles have been 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 Next Big Bull Market Could Be Copper

Source: https://www.wsj.com/articles/the-next-big-bull-market-could-be-copper-a8390fd8?mod=Searchresults_pos5&page=1

From the Article: "Cyclical headwinds could limit gains in 2023, but demand, driven by green power, looks likely to outstrip supply growth"

The Booming Texas Border Town at the Center of a Global Trade Shift

Source: https://www.wsj.com/video/series/in-depth-features/the-booming-texas-border-town-at-the-center-of-a-global-trade-shift/2F243A8C-F9AD-4148-8DB5-B820FA8FF3D1?mod=Searchresults_pos6&page=1

From the Article: "About $800 million worth of products—from auto parts to toys and avocados—passed through Laredo daily in 2022"

U.S. Inflation Forecast to Have Remained Strong in April

Source: https://www.wsj.com/articles/u-s-inflation-forecast-to-have-remained-strong-in-april-1e9a63f3?mod=Searchresults_pos7&page=1

From the Article: "Economists at Bank of America expect no break from inflation in the U.S. when the consumer-price index numbers for April come out Wednesday. They forecast in a note a headline annual price increase at 5%, same as in March.."

Why Is Inflation So Sticky? It Could Be Corporate Profits

Source: https://www.wsj.com/articles/why-is-inflation-so-sticky-it-could-be-corporate-profits-b78d90b7?mod=Searchresults_pos11&page=1

From the Article: "Some companies might have been raising prices faster than their costs have increased"

Pro Take: Fed's Rate Increases Slow U.S. Factories, but Plants Keep Workers

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

Source: https://www.wsj.com/articles/pro-take-feds-rate-increases-slow-u-s-factories-but-plants-keep-workers-b014c52a?mod=Searchresults_pos1&page=2

From the Article: "Some manufacturing surveys are giving off potential recession signals"

China's Consumers Lead Recovery in April

Source: https://www.wsj.com/articles/official-gauge-of-chinas-manufacturing-activity-fell-into-contraction-in-april-2f66258e?mod=Searchresults_pos6&page=2

From the Article: "Retail spending has come back strong, but surveys also showed a surprise contraction in factory activity in April"

Where the Rubber Reads the Road: Tire Makers Aim for Real-Time Data Streams for Autonomous Vehicles

Source: https://www.wsj.com/articles/where-the-rubber-reads-the-road-tire-makers-aim-for-real-time-data-streams-for-autonomous-vehicles-f025a441?mod=Searchresults_pos8&page=2

From the Article: "A tire that could track road conditions in real time would be a 'holy grail' of vehicle control in self-driving cars, says Goodyear's chief technology officer. But the technical difficulties of creating one are high"

Opinion | Russia's Global Food Shortage

Source: https://www.wsj.com/articles/russias-global-food-shortage-exports-europe-eu-crops-ukraine-war-putin-grain-invasion-5b079cf0?mod=Searchresults_pos12&page=2

From the Article: "Ukraine's grain exports keep falling, adding to food insecurity."

Drone Attacks Target Russian Supply Lines Ahead of Ukraine's Expected Offensive

Source: https://www.wsj.com/articles/crescendo-of-attacks-target-russian-supply-lines-ahead-of-expected-offensive-5bd48a28?mod=Searchresults_pos14&page=2

Link back to Table of Contents

From the Article: "Strikes focus on cutting supply routes to Russian forces in southern Ukraine, analysts say"

PacWest Bank Shares Crumble; Maker Limits Obesity Drug Wegovy Supply - What's News - WSJ Podcasts

Source: https://www.wsj.com/podcasts/whats-news/pacwest-bank-shares-crumble-maker-limits-obesity-drug-wegovy-supply/59483981-32e4-4627-b56d-361854ad5a97?mod=Searchresults_pos15&page=2

From the Article: "A.M. Edition for May 4. Shares of regional lender PacWest have tumbled following a report that the bank was considering a sale. WSJ reporter Ben Dummett explains what the news signals about the health of the U.S. banking system."

Oil Prices Under Pressure on Economic Fears and Gusher of Russian Supply

Source: https://www.wsj.com/articles/oil-prices-under-pressure-on-economic-fears-and-gusher-of-russian-supply-c96f7576?mod=Searchresults_pos17&page=2

From the Article: "With a slowing global economy crimping demand, Moscow appears not to have followed through on pledges to cut output"

U.S., Allies Patch Together Ukraine's Defenses Against Russian Warplanes, Missiles

Source: https://www.wsj.com/articles/u-s-allies-patch-together-ukraines-defenses-against-russian-warplanes-missiles-32bb104?mod=Searchresults_pos4&page=3

From the Article: "With missile stocks running low, Kyiv turns to 'MacGyvered' air defenses"

The Green Revolution Is Here. Which Big Miners Are Prepared?

Source: https://www.wsj.com/articles/the-green-revolution-is-here-which-big-miners-are-prepared-e8864ffa?mod=Searchresults_pos17&page=3

From the Article: "New U.S. legislation points to the world being short of copper in a few years. A few big mining firms could be huge beneficiaries."

Link back to Table of Contents

Senate Votes to Disapprove of Biden Solar Tariff Exemption

Source: https://www.wsj.com/articles/bidens-solar-tariff-exemptions-face-disapproval-vote-in-senate-277736f1?mod=Searchresults_pos4&page=4

From the Article: "Some Democrats join Republicans, setting stage for presidential veto"

Reserve Bank of Australia Resumes Interest-Rate Increases

Source: https://www.wsj.com/articles/reserve-bank-of-australia-resumes-interest-rate-increases-6d6261b9?mod=Searchresults_pos8&page=4

From the Article: "SYDNEY—The Reserve Bank of Australia surprised financial markets and raised its official cash rate by 25 basis points to 3.85% after a policy meeting Tuesday, resuming an aggressive campaign of increases. The decision to raise interest rates further comes despite first-quarter consumer-price-index data last week showing inflation likely peaked in late 2022."

Rate Hikes Can Wait

Source: https://www.wsj.com/articles/rate-hikes-can-wait-b54004a5?mod=Searchresults_pos6&page=5

From the Article: "Stress in banking system and debt ceiling risks could make Wednesday's interest rate increase the last for a while"

Opinion | H-1B Visa Shortfall Starves the Economy

Source: https://www.wsj.com/articles/work-visa-shortfall-starves-the-economy-h1b-immigration-high-skill-labor-314e2150?mod=Searchresults_pos7&page=5

From the Article: "Demand for labor has risen steadily since 2004, but the program is still capped at 85,000 a 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.

U.S. Allows Chinese Airlines to Increase Flights to 12 a Week

Source: https://www.wsj.com/articles/u-s-allows-chinese-airlines-to-increase-flights-to-12-a-week-814327a8?mod=Searchresults_pos8&page=5

From the Article: "Passenger flights remain significantly restricted, as bilateral exchanges of people and information dwindle"

WSJ News Exclusive | Shipping Giant Maersk Drops Deep Sea Mining Investment

Source: https://www.wsj.com/articles/shipping-giant-maersk-drops-deep-sea-mining-investment-c226df39?mod=Searchresults_pos12&page=5

From the Article: "Maersk is selling its stake in The Metals Company, the latest big name to divest itself of its seabed mining interests"

Job Openings Near Two-Year Low as Layoffs Jump

Source: https://www.wsj.com/articles/u-s-layoffs-jumped-in-march-as-job-openings-fell-3805c6a1?mod=Searchresults_pos15&page=5

From the Article: "Construction, leisure and hospitality and healthcare cuts drive March increase in layoffs"

Transcript: Fed Chief Powell's Postmeeting Press Conference

Source: https://www.wsj.com/articles/transcript-fed-chief-powells-postmeeting-press-conference-e15c1d7a?mod=Searchresults_pos18&page=5

From the Article: "Federal Reserve Chairman Jerome Powell discussed why the central bank raised interest rates by a quarter percentage point during a press conference after the Fed's policy meeting, and said that decisions regarding further policy tightening would be made on a meeting-by-meeting basis."

Warren Buffett Has Been Betting Big on Oil. It's Time to Find Out Why.

Source: https://www.wsj.com/articles/warren-buffett-oil-stocks-berkshire-hathaway-

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

charlie-munger-2c8b12b8?mod=Searchresults_pos3&page=6

From the Article: "One of the most successful stock pickers of all time admitted years ago that he was 'dead wrong' on an earlier oil-company investment. What's changed? The answer could come this weekend."

Chinese Travelers Swarm Domestic Tourist Sites, a Positive Sign for Economy

Source: https://www.wsj.com/articles/chinese-travelers-swarm-domestic-tourist-sites-a-positive-sign-for-economy-f45c4977?mod=Searchresults_pos8&page=6

From the Article: "Domestic-travel numbers during Labor Day holiday top prepandemic levels"

SEC Buyback-Disclosure Rule Stirs Worry Over Costs and Compliance

Source: https://www.wsj.com/articles/sec-buyback-disclosure-rule-stirs-worry-over-costs-and-compliance-d31548fa?mod=Searchresults_pos14&page=6

From the Article: "Finance executives welcome the effort to improve transparency but question aspects of the requirements and remain concerned over 'undesirable side effects'"

WSJ News Exclusive | China Locks Information on the Country Inside a Black Box

Source: https://www.wsj.com/articles/china-locks-information-on-the-country-inside-a-black-box-9c039928?mod=Searchresults_pos4&page=7

From the Article: "Restrictions on Wind database and other information channels add to campaign to curb foreign influence"

Opinion | Little Lithuania Stands Tall Against Russia and China

Source: https://www.wsj.com/articles/lithuania-stands-against-russia-and-china-landsbergis-taiwan-ukraine-war-362976d3?mod=Searchresults_pos9&page=7

From the Article: "Gabrielius Landsbergis, the Baltic nation's foreign minister, explains

Link back to Table of Contents

why his country never bought into ‘the end of history’ and what Ukraine and Taiwan have in common."

Essay | Iran’s New Friends: Russia and China

Source: https://www.wsj.com/articles/irans-new-friends-russia-and-china-4b2f1f00?mod=Searchresults_pos11&page=7

From the Article: "Having viewed both powers warily for years, the Islamic Republic sees its best prospects for survival as the junior partner in an anti-Western alliance"

WSJ News Exclusive | Google Launches Cybersecurity Certificates for Entry-Level Workers

Source: https://www.wsj.com/articles/google-launches-cybersecurity-certificates-for-entry-level-workers-294e8121?mod=Searchresults_pos1&page=1

From the Article: "Program will teach students the basics of cyber analyst work"

What The Board Needs To Know

Source: https://www.wsj.com/articles/what-the-board-needs-to-know-fbc7263c?mod=Searchresults_pos2&page=1

From the Article: "A weekly cyber risk briefing for corporate board directors."

Patient Drops Request to Compel Hospital Group to Pay Ransom

Source: https://www.wsj.com/articles/patient-drops-request-to-compel-hospital-group-to-pay-ransom-539c9e06?mod=Searchresults_pos4&page=1

From the Article: "A Jane Doe plaintiff had sought to force Lehigh Valley Health Network to meet hackers’ demand for more than $5 million after they posted naked photos of her and other patients"

Link back to Table of Contents

Prosecution of Former Uber Security Chief Carries Warnings for Cyber Leaders

Source: https://www.wsj.com/articles/former-uber-security-chief-gets-probation-in-obstruction-case-87c7c0b9?mod=Searchresults_pos5&page=1

From the Article: "Joseph Sullivan avoids prison sentence while judge puts industry on notice"

New York Attorney General Seeks Broader Authority to Police Crypto

Source: https://www.wsj.com/articles/new-york-attorney-general-seeks-broader-authority-to-police-crypto-cdcf08ed?mod=Searchresults_pos6&page=1

From the Article: "Proposed legislation would require crypto exchanges to have independent public audits of financial statements, among other new requirements"

'THE GODFATHER OF A.I.' LEAVES GOOGLE AND WARNS OF DANGER AHEAD

Source: https://www.nytimes.com/2023/05/01/technology/ai-google-chatbot-engineer-quits-hinton.html?smid=nytcore-ios-share&referringSource=articleShare

From the Article: "But gnawing at many industry insiders is a fear that they are releasing something dangerous into the wild. Generative A.I. can already be a tool for misinformation. Soon, it could be a risk to jobs. Somewhere down the line, tech's biggest worriers say, it could
be a risk to humanity."

Supply Chain Disruptions Should Remind Leaders To Keep Up With Allies

Source: https://www.forbes.com/sites/willyshih/2023/05/01/friend-shoring-means-you-have-to-worry-about-the-health-of-your-friends/

From the Article: "Friend-shoring is a term that has been making the news lately, with the U.S.-Japan trade agreement covering critical minerals being the latest example. It is shorthand for locating supply chains in friendly countries where the political risk to disruption is low."

Link back to Table of Contents

Ransomware Attack On Dallas Disrupts 911, Court And Water Systems - Forbes

Source: https://www.forbes.com/sites/mattnovak/2023/05/04/ransomware-attack-on-dallas-disrupts-911-court-and-water-systems/

From the Article: "Hackers targeting the city of Dallas with ransomware have disrupted the city's 911 computer system, court services and water systems, among a host of other city services. The city first became aware of the attack on Wednesday and it's ongoing at the time of this writing."

CISA Launches New Ransomware Vulnerability Warning Pilot For Critical Infrastructure Entities

Source: https://www.forbes.com/sites/forbestechcouncil/2023/05/01/cisa-launches-new-ransomware-vulnerability-warning-pilot-for-critical-infrastructure-entities/

From the Article: "The U.S. Cybersecurity & Infrastructure Security Agency (CISA) unveiled the Ransomware Vulnerability Warning Pilot (RVWP) program to help ensure critical infrastructure organizations can protect their systems from ransomware attacks."

Lessons From Isaac Asimov on Taming AI

Source: https://www.bloomberg.com/opinion/articles/2023-05-02/what-is-a-safe-ai-chatbot-anthropic-tries-to-have-its-ai-model-tame-itself?re_source=boa_related&leadSource=uverify%20wall

From the Article: "Scientists who broke away from OpenAI say they're creating a safer version of ChatGPT. Co-founder Jared Kaplan explains their approach."

TSMC Plans for First German Chip Fab With Cost Up to €10 Billion

Source: https://www.bloomberg.com/news/articles/2023-05-03/tsmc-plans-for-first-german-chip-fab-with-cost-up-to-10-billion?leadSource=uverify%20wall

From the Article: "TSMC's board could make investment decision in August. Project is seeking state funds to build TSMC's first EU plant."

Link back to Table of Contents

Apple is a Chinese company

Source: https://www.ft.com/content/bf8e3846-2421-4f91-becf-2dfe39ec9941

From the Article: "What happens when the SEC, auditors and investors wake up? Just in recent weeks, China has sanctioned Lockheed Martin and Raytheon; begun a probe of Micron; raided the due diligence firm Mintz Group and arrested some of its staff; detained 17 Japanese businessmen including a senior member of Astellas Pharma; levied a record fine against Deloitte, and amended its espionage law to cover ordinary business activities."

Amazon Web Services sees accelerating ASEAN cloud adoption

Source: https://asia.nikkei.com/Business/Technology/Amazon-Web-Services-sees-accelerating-ASEAN-cloud-adoption

From the Article: "AWS is investing big in the race to develop cloud data centers in Southeast Asia. It announced in March a 25.5 billion ringgit ($6 billion) investment in Malaysia after pouring money into Singapore, Indonesia and Thailand. AWS' investment in Association of Southeast Asian Nations (ASEAN) countries now stands at $22.5 billion."

China's EV industry braces for a shakeout as prices plunge

Source: https://asia.nikkei.com/Business/Business-Spotlight/China-s-EV-industry-braces-for-a-shakeout-as-prices-plunge

From the Article: "Local players face softer demand and competition from foreign makers"

G-7 heads weigh first statement urging China to be 'responsible'

Source: https://asia.nikkei.com/Spotlight/G-7-in-Japan/G-7-heads-weigh-first-statement-urging-China-to-be-responsible

From the Article: "Summit communique to include separate section for Beijing-related concerns"

Link back to Table of Contents

China's espionage law updates undercut courting of investors

Source: https://asia.nikkei.com/Opinion/China-s-espionage-law-updates-undercut-courting-of-investors

From the Article: "Amendments raise concerns on risks involved with data and information handling"

Japan must lead G-7 to address global education crisis

Source: https://asia.nikkei.com/Opinion/Japan-must-lead-G-7-to-address-global-education-crisis

From the Article: "Pandemic has devastated schooling for children in low-income countries"

Sony makes game engine pillar of its EV strategy

Source: https://asia.nikkei.com/Business/Automobiles/Sony-makes-game-engine-pillar-of-its-EV-strategy

From the Article: "Automotive industry shifting focus to value of intangible assets"

To invest in China or not? Milken conference ponders the question

Source: https://asia.nikkei.com/Politics/International-relations/US-China-tensions/To-invest-in-China-or-not-Milken-conference-ponders-the-question

From the Article: "Regulatory crackdowns cited as risk, some say decoupling makes it more attractive"

U.S. to weigh rules for keeping AI safe from China, other competitors

Source: https://asia.nikkei.com/Business/Technology/U.S.-to-weigh-rules-for-keeping-AI-safe-from-China-other-competitors

From the Article: "Biden administration seeks to guard against economic and security

Link back to Table of Contents

risks"

Honda follows Apple model on EVs, working directly with suppliers

Source: https://asia.nikkei.com/Spotlight/Supply-Chain/Honda-follows-Apple-model-on-EVs-working-directly-with-suppliers

From the Article: "New supply chain puts emphasis on batteries, semiconductors"

U.S., Japan and South Korea plan three-way summit in Hiroshima

Source: https://asia.nikkei.com/Politics/International-relations/U.S.-Japan-and-South-Korea-plan-three-way-summit-in-Hiroshima

From the Article: "Biden, Kishida and Yoon to deepen partnership to counter North Korean threat"

Arm's IPO filing fuels speculation of SoftBank going private

Source: https://asia.nikkei.com/Business/Markets/IPO/Arm-s-IPO-filing-fuels-speculation-of-SoftBank-going-private

From the Article: "TOKYO -- Chip design house Arm's application for an initial public offering in the U.S. has rekindled speculation about a long-rumored management buyout of parent SoftBank Group, as the move would vastly expand the Japanese technology group's fundraising power."

NATO to open Japan office, deepening Indo-Pacific engagement

Source: https://asia.nikkei.com/Politics/International-relations/Indo-Pacific/NATO-to-open-Japan-office-deepening-Indo-Pacific-engagement

From the Article: "Two sides to upgrade cooperation on cyber, disruptive tech and disinformation"

Link back to Table of Contents

G-7 can turn the tide on digital trade restrictions

Source: https://asia.nikkei.com/Opinion/G-7-can-turn-the-tide-on-digital-trade-restrictions

From the Article: "Japan's DFFT plan can be foundation for trusted global data sharing"

Huawei diversifies in Vietnam with products for data centers

Source: https://asia.nikkei.com/Business/Technology/Huawei-diversifies-in-Vietnam-with-products-for-data-centers

From the Article: "HO CHI MINH CITY -- Huawei is adding supplies for data centers to its offerings in Vietnam, where storage laws are stoking demand for cloud computing provided by the likes of Amazon Web Services and local unicorn VNG."

Amazon Web Services sees accelerating ASEAN cloud adoption

Source: https://asia.nikkei.com/Business/Technology/Amazon-Web-Services-sees-accelerating-ASEAN-cloud-adoption

From the Article: "AWS is investing big in the race to develop cloud data centers in Southeast Asia. It announced in March a 25.5 billion ringgit ($6 billion) investment in Malaysia after pouring money into Singapore, Indonesia and Thailand. AWS' investment in Association of Southeast Asian Nations (ASEAN) countries now stands at $22.5 billion."

China's EV industry braces for a shakeout as prices plunge

Source: https://asia.nikkei.com/Business/Business-Spotlight/China-s-EV-industry-braces-for-a-shakeout-as-prices-plunge

From the Article: "Local players face softer demand and competition from foreign makers"

G-7 heads weigh first statement urging China to be 'responsible'

Link back to Table of Contents
The articles have been 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://asia.nikkei.com/Spotlight/G-7-in-Japan/G-7-heads-weigh-first-statement-urging-China-to-be-responsible

From the Article: "Summit communique to include separate section for Beijing-related concerns"

China's espionage law updates undercut courting of investors

Source: https://asia.nikkei.com/Opinion/China-s-espionage-law-updates-undercut-courting-of-investors

From the Article: "Amendments raise concerns on risks involved with data and information handling"

Japan must lead G-7 to address global education crisis

Source: https://asia.nikkei.com/Opinion/Japan-must-lead-G-7-to-address-global-education-crisis

From the Article: "Pandemic has devastated schooling for children in low-income countries"

Sony makes game engine pillar of its EV strategy

Source: https://asia.nikkei.com/Business/Automobiles/Sony-makes-game-engine-pillar-of-its-EV-strategy

From the Article: "Automotive industry shifting focus to value of intangible assets"

To invest in China or not? Milken conference ponders the question

Source: https://asia.nikkei.com/Politics/International-relations/US-China-tensions/To-invest-in-China-or-not-Milken-conference-ponders-the-question

From the Article: "Regulatory crackdowns cited as risk, some say decoupling makes it more attractive"

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

U.S. to weigh rules for keeping AI safe from China, other competitors

Source: https://asia.nikkei.com/Business/Technology/U.S.-to-weigh-rules-for-keeping-AI-safe-from-China-other-competitors

From the Article: "Biden administration seeks to guard against economic and security risks"

Honda follows Apple model on EVs, working directly with suppliers

Source: https://asia.nikkei.com/Spotlight/Supply-Chain/Honda-follows-Apple-model-on-EVs-working-directly-with-suppliers

From the Article: "New supply chain puts emphasis on batteries, semiconductors"

U.S., Japan and South Korea plan three-way summit in Hiroshima

Source: https://asia.nikkei.com/Politics/International-relations/U.S.-Japan-and-South-Korea-plan-three-way-summit-in-Hiroshima

From the Article: "Biden, Kishida and Yoon to deepen partnership to counter North Korean threat"

Arm's IPO filing fuels speculation of SoftBank going private

Source: https://asia.nikkei.com/Business/Markets/IPO/Arm-s-IPO-filing-fuels-speculation-of-SoftBank-going-private

From the Article: "TOKYO -- Chip design house Arm's application for an initial public offering in the U.S. has rekindled speculation about a long-rumored management buyout of parent SoftBank Group, as the move would vastly expand the Japanese technology group's fundraising power."

NATO to open Japan office, deepening Indo-Pacific engagement

Source: https://asia.nikkei.com/Politics/International-relations/Indo-Pacific/NATO-to-

Link back to Table of Contents

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

open-Japan-office-deepening-Indo-Pacific-engagement

From the Article: "Two sides to upgrade cooperation on cyber, disruptive tech and disinformation"

G-7 can turn the tide on digital trade restrictions

Source: https://asia.nikkei.com/Opinion/G-7-can-turn-the-tide-on-digital-trade-restrictions

From the Article: "Japan's DFFT plan can be foundation for trusted global data sharing"

Huawei diversifies in Vietnam with products for data centers

Source: https://asia.nikkei.com/Business/Technology/Huawei-diversifies-in-Vietnam-with-products-for-data-centers

From the Article: "HO CHI MINH CITY -- Huawei is adding supplies for data centers to its offerings in Vietnam, where storage laws are stoking demand for cloud computing provided by the likes of Amazon Web Services and local unicorn VNG."

Link back to Table of Contents