Weekly Security Articles 03-November-2021

Contents

Link back to Table of Contents

Link back to Table of Contents

Link back to Table of Contents

Link back to Table of Contents

Contribution Managers:
Christopher Sundberg
Kirsten Koepsel
Daniel DiMase
Ann Marie van den Hurk

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 G32CPSS@sae.org along with the URL for the document.

Events

National Microelectronics Security Training Center

Various dates in October and November 2021

Source: https://mestcenter.org/index.php/webinars/

NIST Workshop on EO 14028: Guidelines for Enhancing Software Supply Chain Security

November 8, 2021

From the webpage: “The workshop will share and discuss the approach that NIST is taking to support Section 4e of Executive Order 14028.

NIST has released the Draft Special Publication (SP) 800-218, Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities. The SSDF is a set of fundamental, sound practices for secure software development based on established standards and guidelines produced by various organizations. The SSDF directly addresses several practices that were called out in Section 4e. The SSDF also provides a starting point for discussing other practices that Section 4e specifies.

To support this discussion, NIST is soliciting input about the types of meaningful artifacts of secure software development that software producers can share publicly with software acquirers. This workshop will bring together experts with different viewpoints to share their insights on producing and sharing artifacts of secure software development tools and processes, as well as on attesting to following specific secure software development practices. ”

Source: https://www.nist.gov/news-events/events/2021/11/executive-order-14028-guidelines-%03enhancing-software-supply-chain

16th Annual API Cybersecurity Conference for the OIl & Natural Gas Industry

Nov 9-10, 2021, The Woodlands, TX (and virtual)
From the webpage: “ 60 presentations in 3 tracks...conference is expected to host over 600 cybersecurity experts from the oil and gas industry ”

Source: https://www.api.org/products-and-services/events/calendar/2021/cyber

Link back to Table of Contents

Escar Europe (Automotive Cyber Security Conference)

Nov 10-11, 2021

From the webpage: “Modern cars have become complex digital devices and automotive Cyber Security is one of the most important issues. Therefore, the overall goal and objective of escar is to provide a forum for collaboration among private industry, academia, and government regarding modern in-vehicle Cyber Security threats, vulnerabilities, and risk mitigation/countermeasures. escar offers an opportunity for information exchange, networking and is a platform to define research needs. International and high-quality speakers give recent insights and encourage discussions.”

Source: https://www.escar.info/escar-europe.html

CPSIoTSec 2021

Nov 15, 2021; Seoul, South Korea

From the website: “The Joint Workshop on CPS&IoT Security and Privacy (CPSIoTSec) is the result of the merger of the Workshop on Cyber-Physical Systems Security and Privacy (CPS-SPC) and Workshop on the Internet of Things Security and Privacy (IoTS&P) previously organized annually in conjunction with ACM Conference on Computer and Communications Security.”

Call for papers: Deadlines: Submission deadline: June 25, 2021 (23:59 Anywhere on Earth) Submission deadline applicable only to papers rejected from ACM CCS 2021: July 30, 2021 (23:59 Anywhere on Earth) Notification of acceptance/rejection (tentative): August 13, 2021 Deadline for submission of camera-ready papers (hard deadline): September 6, 2021

Source: https://cpsiotsec.github.io/

IEEE International Conference on Physical Assurance and Inspection of Electronics (PAINE)

November 30 – December 2, 2021

From the website: “Physical inspection of electronics have grown significantly over the past decade and is becoming a major focus for the chip designers, original equipment manufacturers, and system developers. The complex long life of the electronic devices coupled with their diverse applications are making them increasingly vulnerable to various forms of threats and inspection. Large industry and government efforts have been put in place across the globe to address related supply chain security problems to offer solutions, training and services. The number of programs introduced by US government have increased over the years to analyze and develop relevant solutions. Although much focus is given to digital domain, physical assurance and inspection of electronics as well as physical fingerprinting based on analog parameters are rapidly providing opportunities for unique countermeasures.

PAINE conference provides a unique venue to all researchers and practitioners from academia, industry, and government to have productive dialog on such topics. The papers accepted for publication in PAINE will appear in IEEE Xplore Digital Library. PAINE covers the broad topic of hardware security and trust, example topics of interest include but not limited to:

Topics to be Covered:

- Security primitives: Novel devices, materials, and systems
- Trojans and backdoors: Detection and prevention
- Fault injection assessment and countermeasures
- Side channel assessment (power, timing, EM) for assurance and countermeasures
- Analog & mixed-signal circuits and systems security
- FPGA Bitstream protection and vulnerabilities
- Emerging topics in physical inspection and assurance
- Counterfeit Detection and Anti-Counterfeit Technique
- Image analysis and artificial intelligence for assurance and inspection
- Novel material and devices for assurance
- Sample Preparation
- PCB trust and assurance
- Chip and PCB level decomposition for assurance
- FIB/SEM for assurance
- Electro-optical probing using PEM, EOP, EOFM, etc.
- Physical/side channel fingerprinting
- Mod-chip on PCB
- Microprobing and nanoprobing
- Bus-snooping
- Field-based weakness
- Countermeasures against tampering and decomposition
- Physical/logical shielding etc.”

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

Security Weekly Unlocked

December 5-8, 2021

From the website: “In true Security Weekly fashion, we like to do things a bit differently, so we’re giving this conference an “anti-con” structure, with a strong focus on community building and networking with other security professionals face-to-face. Presentations will be staggered throughout six communities, giving attendees the opportunity to visit them all.The relaxed, laid-back environment of this event will allow you the opportunity to reconnect with old friends, meet new friends, and make the most of your time, without having to worry about missing presentations in competing tracks.”

Source: https://events.securityweekly.com/unlocked2021/1233293?ref=SWCFP

Call for Papers:
https://events.securityweekly.com/unlocked2021/callforpapers?ref=SWCFP

Design Automation Conference

December 5-9, 2021

From the website: “The Design Automation Conference (DAC) is recognized as the premier conference for design and automation of electronic systems. DAC offers outstanding training, education, exhibits and superb networking opportunities for designers, researchers, tool developers and vendors.

Members are from a diverse worldwide community of more than 1,000 organizations that attend each year, represented by system designers and architects, logic and circuit designers, validation engineers, CAD managers, senior managers and executives, and researchers and academicians from leading universities.

Close to 300 technical presentations and sessions are selected by a committee of electronic design experts offer information on recent developments and trends, management practices and new products, methodologies and technologies.

A highlight of DAC is its exhibition and suite area with approximately 200 of the leading and emerging companies in:

- Artificial Intelligence/ Machine Learning (AI/ ML)
- Automotive
- Design Services
- Design on Cloud
- Electronic Design Automation (EDA)
- Embedded Systems and Software (ESS)
- Intellectual Property (IP)
- Security/Privacy

The conference is sponsored by the Association for Computing Machinery (ACM) and the Institute of Electrical and Electronics Engineers (IEEE), and is supported by ACM's Special Interest Group on Design Automation (SIGDA)."

Source: https://www.dac.com/

NDIA 2021 Virtual Systems & Mission Engineering Conference

December 6-8, 2021

From the website: "Join us for the NDIA's second virtual Systems and Mission Engineering Conference. While we are no longer able to meet in person for the 24th Annual Systems and Mission Engineering Conference, we are excited to bring you the same great content you can expect at an in-person conference - all from the comfort of your home or office! Stay tuned for an agenda and other details.

Why Attend?

- Gain insight on improving acquisition and performance of defense programs and systems.
- Hear from Program Managers, Systems Engineers, Chief Scientists, and Engineers and Managers.
- Participate in Q&As with session speakers; getting your most pressing systems engineering questions answered.
- View handouts to supplement and enhance your virtual experience.
- Network and build relationships with like-minded professionals during virtual networking opportunities.

Source: https://www.ndia.org/events/2021/12/6/24th-sme-conference-virtual

IEEE International Symposium on Hardware Oriented Security and Trust (HOST)

December 12-15, 2021

From the website: “Rapid proliferation of computing and communication systems with increasing computational power and connectivity into every sphere of modern life has brought security to the forefront of system design, test, and validation processes. The emergence of new application spaces for these systems in the internet-of-things (IoT) regime is creating new attack surfaces as well as new requirements for secure and trusted system operation. Additionally, the design, manufacturing and the distribution of microchip, PCB, as well as other electronic components are becoming more sophisticated and globally distributed with a number of potential security vulnerabilities. Therefore, hardware plays an increasingly important and integral role in system security with many emerging system and application vulnerabilities and defense mechanisms relating to hardware. IEEE International Symposium on Hardware Oriented Security and Trust (HOST) aims to facilitate the rapid growth of hardware-based security research and development. HOST highlights new results in the area of hardware and system security. Relevant research topics include techniques, tools, design/test methods, architectures, circuits, and applications of secure hardware.

Call for Paper
HOST 2021 invites original contributions in all areas of overlap between hardware and security. This includes but is not limited to the following:

Hardware

- Security primitives
- Computer-aided design (CAD) tools
- Emerging and nanoscale devices
- Trojans and backdoors
- Side-channel attacks and mitigation
- Fault injection and mitigation
- (Anti-)Reverse engineering and physical attacks
- Anti-tamper
- Anti-counterfeit
- Hardware Obfuscation

Architecture

- Trusted execution environments
- Cache-side channel attacks and mitigation
- Privacy-preserving computation
- System-on-chip (SoC)/platform security
- FPGA and reconfigurable fabric security
- Cloud computing
- Smart phones and smart devices

System

- Internet-of-things (IoT) security

- Sensors and sensor network security
- Smart grid security
- Automotive/autonomous vehicle security
- Cyber-physical system security
- (Adversarial) Machine learning and cyber deception
- Security and trust for future pandemics
- Blockchain and cryptocurrencies"

Source: http://www.hostsymposium.org/

PARTS AND MATERIAL MANAGEMENT CONFERENCE

IMPORTANT UPDATE - PMMC 2021 is POSTPONED until Spring of 2022

From the website: "Is your program having problems with DMSMS and obsolescence? Are the problems getting worse? Do you have questions about intellectual property rights, additive manufacturing, cyber security, and counterfeit prevention? Do you want to meet DMSMS and parts management experts who can help improve your situation?

Last year has been a time of important and positive changes for the DoD DMSMS and parts management communities. In the closing months of 2020, DoDI 4245.15, DoD DMSMS Management was published. This is the first DoD DMSMS instruction in more than 40 years! In addition, DoDI 5000.88, Engineering of Defense Systems which includes a requirement to implement parts management processes was also published.

The 2021 Parts and Materials Management Conference provides you with new information to successfully meet these new requirements, shows what is happening in the DMSMS community, and addresses your questions. You will have opportunities to interact and exchange ideas with specialists from government, industry, and academia, express your views and ideas on improving DMSMS and parts management, and meet with technical experts. You will experience state of the art technologies that can be applied to parts and material management at the training sessions and the exhibit hall.

Attendees will have the opportunity to participate in informative training, dynamic plenary talks, and technical breakout sessions to exchange information and perspectives on a wide variety of topics including:

- DMSMS and parts management best practices and lessons learned, strategic activities, data sharing and commonality, contract language, programming and budgeting, metrics, technology refresh, and technology roadmaps.

- Intellectual property (IP) and technical data management (TDM) for DMSMS and parts management, IP/TDM solutions, and methods of resolving IP/TDM issues.
- Counterfeit parts and materials risks and impacts, best practices, proactive planning, parts monitoring, and issues resolutions.
- Additive manufacturing (AM) case studies, current state AM, new AM technologies, and challenges in leveraging AM for obsolete parts
- Cyber physical systems security threats and mitigations, software and hardware assurance and components selection, security gaps, monitoring, and electronic & physical security
- Supply chain risk management processes and tools, ownership of critical technologies, impact of recent events (COVID-19), and policy regarding foreign sources
- Updates on the latest DMSMS and Parts Management policies recently issued including DoDI 4245.15, DoDI 5000.88, SD-19, SD-22, and SD-26.

Source: http://www.pmmcmeeting.org/

Request for Comments

Notice of Request for Public Comments on Risks in the Information Communications Technology Supply Chain

Comments due November 4, 2021

From the article: “The departments of Commerce and Homeland Security are looking to incorporate comments on cybersecurity design details into a report on the supply of information and communications technology required by executive order.”

Federal Register Notice: https://www.federalregister.gov/documents/2021/09/20/2021-20229/notice-of-request-for-public-comments-on-risks-in-the-information-communications-technology-supply

Source: https://www.nextgov.com/cybersecurity/2021/09/agencies-seek-comments-supply-chain-security-critical-software/185472/

Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities

Comments due November 5, 2021

From the article: “This document will replace the NIST Cybersecurity White Paper released in April 2020 which defined the original Secure Software Development Framework (SSDF), and it includes a change log summarizing the major changes from the April 2020 version. NIST used inputs from the public and its June 2021 workshop to shape SSDF version 1.1 in support of NIST's responsibilities under Executive Order (EO) 14028. The new SSDF draft also includes mappings from EO 14028 clauses to the SSDF practices and tasks that help address each clause."

Source: https://csrc.nist.gov/publications/detail/sp/800-218/draft

Protecting Information and System Integrity in Industrial Control System Environments: Cybersecurity for the Manufacturing Sector

Comments due November 7, 2021

From the article: "Draft NIST SP 1800-10 provides a practical example solution to help manufacturers protect their Industrial Control Systems (ICS) from data integrity attacks. Manufacturers are increasingly relying on ICS to monitor and control physical processes to produce goods for public consumption. ICS has also helped manufacturers boost productivity, but it has made them more vulnerable to cyber threats such as malware, malicious insider activity, even human error. As technology and operations become more integrated, manufacturers can use this guide to improve their security, reduce the likelihood of data integrity breaches, and better protect their operating systems."

Draft for comment: https://csrc.nist.gov/publications/detail/sp/1800-10/draft

Source: https://www.nist.gov/news-events/news/2021/09/dhs-nist-coordinate-releasing-preliminary-cybersecurity-performance-goals

Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (2nd Draft)

Comments due: December 3, 2021

From the article: "We worked on making the implementation guidance more consumable by different audiences by revising the structure of the document and adding Audience Profiles. We also added two NEW appendices focused more specifically on Federal departments and agencies."

Source: https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/draft

Hardware-Enabled Security: Enabling a Layered Approach to Platform Security for Cloud and Edge Computing Use Cases (2nd Draft)

Comments due: December 6, 2021

From the article: “The National Cybersecurity Center of Excellence (NCCoE) has released three new draft reports on hardware-enabled security and trusted cloud for public comment. The foundation of any cloud data center or edge computing security strategy should be securing the platform on which data and workloads will be executed and accessed. The physical platform provides the initial protections to help ensure that higher-layer security controls can be trusted.”

Note this request covers 3 documents and all comments are due December 6, 2021.

Source: https://csrc.nist.gov/publications/detail/nistir/8320/draft

Hardware-Enabled Security: Policy Based Governance in Trusted Container Platforms

Comments due December 6, 2021

From the article: “The National Cybersecurity Center of Excellence (NCCoE) has released three new draft reports on hardware-enabled security and trusted cloud for public comment. The foundation of any cloud data center or edge computing security strategy should be securing the platform on which data and workloads will be executed and accessed. The physical platform provides the initial protections to help ensure that higher-layer security controls can be trusted.”

Note this request covers 3 documents and all comments are due December 6, 2021.

Source: https://csrc.nist.gov/publications/detail/nistir/8320b/draft

DRAFT Baseline Criteria for Consumer Software CybersecurityLabeling

Comments due: December 16, 2021

From the article: “In an effort to improve consumers’ ability to make informed decisions about software they purchase, the National Institute of Standards and Technology (NIST) has drafted a set of cybersecurity criteria for consumer software. The criteria are intended to aid in the development and voluntary use of labels to indicate that the software incorporates a baseline level of security measures.”

Source: https://www.nist.gov/news-events/news/2021/10/nist-seeks-public-input-consumer-software-labeling-cybersecurity

Link to draft:
https://www.nist.gov/system/files/documents/2021/11/01/Draft%20Consumer%20Software%20Labeling.pdf

NIST Risk Management Framework RMF

NIST SP 800-53 Public Comment website

From the webpage: “The NIST SP 800-53 Public Comment Site was developed to ensure that the SP 800-53 control catalog provides the most comprehensive and up-to-date set of controls/countermeasures to manage security, privacy, and supply chain risk. By modernizing the NIST comment process and moving to an online dataset instead of following a document-based update process, NIST can provide its stakeholders the most up-to-date controls in multiple data formats to manage risk while encouraging use of automation.”

Source: https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/public-comments-home

Trusted Cloud: Security Practice Guide for VMware Hybrid Cloud Infrastructure as a Service (IaaS) Environments

Comments due December 6, 2021

From the article: “The National Cybersecurity Center of Excellence (NCCoE) has released three new draft reports on hardware-enabled security and trusted cloud for public comment. The foundation of any cloud data center or edge computing security strategy should be securing the platform on which data and workloads will be executed and accessed. The physical platform provides the initial protections to help ensure that higher-layer security controls can be trusted."

Note this request covers 3 documents and all comments are due December 6, 2021.

Source: https://csrc.nist.gov/publications/detail/sp/1800-19/draft

Patches/Advisories

Review - 1 Advisory Published – 10-26-21

Source: https://chemical-facility-security-news.blogspot.com/2021/10/review-1-advisory-published-10-26-21.html

B. Braun Infusomat Space Large Volume Pump

Source: https://us-cert.cisa.gov/ics/advisories/icsma-21-294-01

ICONICS GENESIS64 and Mitsubishi Electric MC Works64

Source: https://us-cert.cisa.gov/ics/advisories/icsa-21-294-01

Delta Electronics DIALink

Source: https://us-cert.cisa.gov/ics/advisories/icsa-21-294-02

ICONICS GENESIS64 and Mitsubishi Electric MC Works64 OPC UA

Source: https://us-cert.cisa.gov/ics/advisories/icsa-21-294-03

NOBELIUM Attacks on Cloud Services and other Technologies

Source: https://us-cert.cisa.gov/ncas/current-activity/2021/10/25/nobelium-attacks-cloud-services-and-other-technologies

Malware Discovered in Popular NPM Package, ua-parser-js

Source: https://us-cert.cisa.gov/ncas/current-activity/2021/10/22/malware-discovered-popular-npm-package-ua-parser-js

Cisco Releases Security Updates for Multiple Products

Source: https://us-cert.cisa.gov/ncas/current-activity/2021/10/28/cisco-releases-security-updates-multiple-products

2021 CWE Most Important Hardware Weaknesses

Source: https://us-cert.cisa.gov/ncas/current-activity/2021/10/28/2021-cwe-most-important-hardware-weaknesses

Fuji Electric Tellus Lite V-Simulator and V-Server Lite

Source: https://us-cert.cisa.gov/ics/advisories/icsa-21-299-01

ISC Releases Security Advisory for BIND

Source: https://us-cert.cisa.gov/ncas/current-activity/2021/10/28/isc-releases-security-advisory-bind

Review - Public ICS Disclosures – Week of 10-23-21 – Part 1

Source: https://chemical-facility-security-news.blogspot.com/2021/10/review-public-ics-disclosures-week-of_30.html

Google Releases Security Updates for Chrome

Source: https://us-cert.cisa.gov/ncas/current-activity/2021/10/29/google-releases-security-updates-chrome

GoCD Authentication Vulnerability

Source: https://us-cert.cisa.gov/ncas/current-activity/2021/10/29/gocd-authentication-vulnerability

Review - Public ICS Disclosures – Week of 10-23-21 – Part 2

Source: https://chemical-facility-security-news.blogspot.com/2021/10/review-public-ics-disclosures-week-of_31.html

Review - 1 Advisory and 2 Updates Published – 10-28-21

Source: https://chemical-facility-security-news.blogspot.com/2021/10/review-1-advisory-and-2-updates.html

Sensormatic Electronics victor

Source: https://us-cert.cisa.gov/ics/advisories/icsa-21-301-01

Multiple vulnerabilities in wolfSSL

Source: https://www.cybersecurity-help.cz/vdb/SB2021110215

Privilege escalation in Tenable Nessus

Source: https://www.cybersecurity-help.cz/vdb/SB2021110115

Improper input validation in Unicode Bidirectional Algorithm

Source: https://www.cybersecurity-help.cz/vdb/SB2021110201

Improper input validation in Unicode character definitions

Source: https://www.cybersecurity-help.cz/vdb/SB2021110202

Podcasts/Videos

Changes Coming to CMMC & DoD Cybersecurity: Part 1 of 2

Source: https://www.youtube.com/watch?v=XpECAE--o7Y

Changes Coming to CMMC & DoD Cybersecurity: Part 2

Source: https://www.youtube.com/watch?v=mU03zvjwsnE

Safeguarding electric infrastructure takes center stage at DOE's inaugural SEAB meeting

Industrial Cyber has an excellent summary of the initial SEAB (Secretary of Energy Advisory Board) meeting that took place on 28-Oct-2021. Several industry experts gave testimony to Sec. Granholm on the current state of cybersecurity in the United States electric infrastructure. The SEAB is purely advisory in nature. Several cybersecurity recommendations were made by experts:

* Out of band process sensor monitoring

* Suggested DOE emergency order for Cybersecurity protections/hardening (including physical security, EMP/GMD, and severe weather events)

* Whistleblower protections for workers in energy infrastructure similar to same protections enjoyed by nuclear workers

A recording of the SEAB meeting can be found here: https://www.energy.gov/seab/seab-meetings

Source: https://industrialcyber.co/article/safeguarding-electric-infrastructure-takes-center-stage-at-does-inaugural-seab-meeting/

Reports

Reading INTERPOL the African Cyberthreat Assessment Report 2021

From the article: "INTERPOL published the African Cyberthreat Assessment Report 2021, a report that analyzes evolution of cybercrime in Africa."

Source: https://securityaffairs.co/wordpress/123959/cyber-crime/interpol-the-african-cyberthreat-assessment-report-2021.html

Hackers-for-Hire drive the Evolution of the New ENISA Threat Landscape

Summary: ENISA Threat Landscape report for 2021 has been released.
Link to report: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

Source: https://www.enisa.europa.eu/news/enisa-news/hackers-for-hire-drive-the-evolution-of-the-new-enisa-threat-landscape

Additional sources: https://securityaffairs.co/wordpress/123839/security/enisa-threat-landscape-report-2021.html

2021 CWE Most Important Hardware Weaknesses

Summary: CISA announces MITRE's 2021 CWE centering on hardware.
Source: https://cwe.mitre.org/scoring/lists/2021_CWE_MIHW.html

Source: https://us-cert.cisa.gov/ncas/current-activity/2021/10/28/2021-cwe-most-important-hardware-weaknesses

NTIA makes significant changes for development of a model for SBOMs, including software components

Summary: : Framing Software Component Transparency: Establishing a Common Software Bill of Materials (SBOM);
From the announcement: "The document adds a timestamp to baseline attributes, provides clarified requirements aspects of baseline attributes, and adds CycloneDX as an additional format. It also removes some existing formats and has been renumbered accordingly. The NTIA record has also updated language in baseline attributes and terminology, updated and harmonized language across working groups, with modernized figures and tables, and has made various editorial improvements and clarifications."
Link:
https://ntia.gov/files/ntia/publications/ntia_sbom_framing_2nd_edition_20211021.pdf

Source: https://industrialcyber.co/article/ntia-makes-significant-changes-for-development-of-a-model-for-sboms-including-software-components/

Link back to Table of Contents

Excerpt: LOGIIC's Project 12 Safety Instrumentation Report - InTech

Summary: LOGIIC's SIS report for security in Oil and Gas. From the webite: "The Linking the Oil and Gas (O&G) Industry to Improve Cybersecurity (LOGIIC) consortium was established in partnership with the U.S. Department of Homeland Security (DHS) Science and Technology (S&T) Directorate to review and study cybersecurity issues in industrial control systems (ICS) that impact safety and business performance as they pertain to the O&G sector. Project 12 was conducted during 2020 and focused on the security and management of safety instrumentation. The project revealed numerous consequential and recurring findings that indicate a pervasive industry-wide security problem in safety systems. This report documents key findings and recommendations for asset owners, vendors, and standards bodies."
Link:https://isaorgwebsite.blob.core.windows.net/media/isa/media/pdf/logiic/logiic-project-12-final-report.pdf

Source: https://gca.isa.org/blog/excerpt-logiic-safety-instrumentation-report

Cyberthreat Defense Report | (ISC)²

Summary: 2021 (ISC)2 Cyberthreat Defense Report From the From the article: "ISC)² is proud to sponsor CyberEdge's 2021 Cyberthreat Defense Report and arm you with key insights for the future. Now in its eighth year, this report provides a comprehensive review of the perceptions of 1,200 IT security professionals representing 17 countries and 19 industries. Findings include: A record 86% of organizations suffered from a successful cyberattack last year. The vast majority (87%) of organizations are experiencing an IT security skills shortfall. Nearly all respondents (99%) agreed that achieving a cybersecurity certification would help their careers; the top choices were cloud security, software security, and security administration 41% of security applications are delivered via the cloud, up from 36% last year."
Link: https://www.isc2.org/landing/cyberthreat-defense-report

Source: https://www.isc2.org/landing/cyberthreat-defense-report

Upstream Security 2021 Cyberthreat Report

From the website: “This 2021 Global Automotive Cybersecurity report includes an in-depth analysis of the cyber threat landscape over the last decade, with an emphasis on 2020. Upstream Security’s research team classified and analyzed hundreds of publicly reported incidents, and for the first-time-ever, mapped cyber incidents according to the UNECE WP.29 threat categories and dived into non-disclosed incidents found on the deep and dark web.
This Global Automotive Cybersecurity Report includes:

- Cyber threat trends over the last decade, highlighting 2020
- Details and analysis of 200+ cyber incidents from 2020
- ISO/SAE 21434 standard and UNECE WP.29 regulation in practice
- A dive into real-life deep and dark web automotive cyber attacks
- Current automotive cybersecurity solutions incorporated in the industry“

Link: https://upstream.auto/2021report/

CISA RELEASES DIRECTIVE ON REDUCING THE SIGNIFICANT RISK OF KNOWN EXPLOITED VULNERABILITIES

From the announcement: "CISA issued BOD 22-01 to drive federal agencies to mitigate actively exploited vulnerabilities on their networks, sending a clear message to all organizations across the country to focus patching on the subset of vulnerabilities that are causing harm now, and enable CISA to drive continuous prioritization of vulnerabilities based on our understanding of adversary activity. The Directive applies to all software and hardware found on federal information systems, including those managed on agency premises or hosted by third parties on an agency's behalf. With this Directive, CISA is imposing the first government-wide requirements to remediate vulnerabilities affecting both internet-facing and non-internet facing assets."

Link: https://cyber.dhs.gov/bod/22-01/

Announcement: https://www.cisa.gov/news/2021/11/03/cisa-releases-directive-reducing-significant-risk-known-exploited-vulnerabilities

TROJAN SOURCE

'Trojan Source' Bug Threatens the Security of All Code

Summary: Slashdot discussion about the Trojan Source bug.

Source: https://it.slashdot.org/story/21/11/01/2147254/trojan-source-bug-threatens-the-security-of-all-code

Hiding Vulnerabilities in Source Code

Summary: Bruce Schneier with links to the "Trojan Source" vulnerability that essentially allows an attacker to place vulnerabilities in code using the 'encoding layer'; invisible to the human reader.

Source: https://www.schneier.com/blog/archives/2021/11/hiding-vulnerabilities-in-source-code.html

Trojan Source Attacks

Summary: OSS (Open Source Security) bulletin on the 'Trojan Source' attacks

Source: http://seclists.org/oss-sec/2021/q4/80

Hackers Can Hide Security Flaws in Source Code Using New' Trojan Source' Technique

Summary: CyberIntel magazine does in depth on the Trojan Source vulnerability and how it can be exploited.

Source: https://cyberintelmag.com/malware-viruses/hackers-can-hide-security-flaws-in-source-code-using-new-trojan-source-technique/

IRAN FUEL DISTRIBUTION

Iran Struggles to Relaunch Petrol Stations After Cyberattack

From the article: "Iran struggled Wednesday to restart its petrol distribution system after it was hit by an unprecedented cyber-attack which security officials said was launched from abroad. The unclaimed attack crippled the country's system of government-issued electronic cards which motorists use to purchase heavily subsidised fuel. Long queues have formed outside petrol stations, angering motorists in a country already suffering under tough economic sanctions over its nuclear dispute with major powers."

Source: https://www.securityweek.com/iran-struggles-relaunch-petrol-stations-after-cyberattack

After The Distribution Network In Iran Being hacked, All Gas Stations Out Of Service

Summary: More on the Iranian petrol distribution network attack. Similar to the railway system attack earlier this year

Source: https://cyberintelmag.com/attacks-data-breaches/after-the-distribution-network-in-iran-being-hacked-all-gas-stations-out-of-service/

Iranian state media blames hack for apparent fuel shortage, the latest incident to draw attention

From the article: "Iranian officials say a cyberattack has forced the temporary closure of a government system that manages fuel subsidies, rendering it difficult for many citizens to refuel their cars."

Source: https://www.cyberscoop.com/iran-gas-hack-fuel-breach/

Additional sources:
https://www.securityweek.com/iran-blames-cyberattack-fuel-supply-hit

https://threatpost.com/cyber-attack-cripples-iranian-fuel-distribution-network/175794/

https://www.bleepingcomputer.com/news/security/iranian-gas-stations-out-of-service-after-distribution-network-hacked/

https://www.darkreading.com/attacks-breaches/gas-stations-in-iran-downed-by-cyberattack-reports https://www.securityweek.com/many-ransomware-attacks-ot-organizations-involved-ryuk-ibm

https://securityaffairs.co/wordpress/123824/hacking/iranian-gas-stations-incident.html

Articles of Interest

Russia-linked Nobelium APT targets orgs in the global IT supply chain

From the article: "Russia-linked Nobelium APT group has breached at least 14 managed service providers (MSPs) and cloud service providers since May 2021."

Source: https://securityaffairs.co/wordpress/123754/apt/nobelium-apt-it-supply-chain.html

Additional sources:
https://www.theregister.com/2021/10/25/nobelium_russia_svr_msp_warning_microsoft/

https://cyberintelmag.com/attacks-data-breaches/microsoft-says-russian-svr-hacked-at-least-14-supply-chain-firms-since-may/

https://securityintelligence.com/nobelium-espionage-campaign-persists/

https://www.bleepingcomputer.com/news/microsoft/microsoft-russian-svr-hacked-at-least-14-it-supply-chain-firms-since-may/

https://www.zdnet.com/article/solarwinds-hacking-group-nobelium-is-now-targeting-the-global-it-supply-chain-microsoft-warns/

https://www.schneier.com/blog/archives/2021/10/more-russian-svr-supply-chain-attacks.html

https://www.securityweek.com/russia-linked-solarwinds-hackers-continue-launching-supply-chain-attacks

https://www.cyberscoop.com/?p=59745

https://www.darkreading.com/attacks-breaches/solarwinds-attacker-targets-cloud-service-providers-in-new-supply-chain-threat https://www.protocol.com/bulletins/russian-hackers-targeted-tech-companies

https://www.csoonline.com/article/3638452/russian-cyberspies-target-cloud-services-providers-and-resellers-to-abuse-delegated-access.html

A Russian-speaking ransomware gang says it hacked the National Rifle Association

From the article: "A ransomware group known as Grief claimed on Wednesday to have hacked the National Rifle Association, releasing 13 documents allegedly belonging to the organization and threatening to release more if the NRA doesn't pay an extortion fee of an undisclosed sum."

Source: https://www.cyberscoop.com/evil-corp-nra-ransomware/

Additional sources:
https://go.theregister.com/feed/www.theregister.com/2021/10/28/grief_ransomware_gang_nra/

https://www.securityweek.com/ransomware-gang-claims-have-stolen-data-national-rifle-association

https://www.bleepingcomputer.com/news/security/nra-no-comment-on-russian-ransomware-gang-attack-claims/

https://cyberintelmag.com/attacks-data-breaches/no-reaction-from-the-nra-on-accusations-of-a-russian-ransomware-gang-attack/

https://securityaffairs.co/wordpress/123849/cyber-crime/grief-ransomware-hit-nra.html

https://threatpost.com/grief-ransomware-nra/175850/

Feds cuff Russian said to be developer of 'Trickbot' ransomware

From the article: "The US Department of Justice claims it's arrested a member of a gang that deployed the Trickbot ransomware...."

Source: https://www.theregister.com/2021/10/29/trickbot_arrest/

Additional sources:
https://www.securityweek.com/russian-man-extradited-us-role-trickbot-malware-development

https://www.bleepingcomputer.com/news/security/trickbot-malware-dev-extradited-to-us-faces-60-years-in-prison/

https://cyberintelmag.com/malware-viruses/creator-of-the-trickbot-virus-extradited-to-the-us-faces-maximum-sentence-of-60-years/

https://www.cyberscoop.com/russian-national-allegedly-behind-trickbot-malware-extradited-to-us-makes-court-appearance/

https://www.darkreading.com/attacks-breaches/russian-national-accused-of-role-in-trickbot-is-extradited-to-us

https://securityaffairs.co/wordpress/123940/cyber-crime/trckbot-russian-member-extradicted.html

Mozilla blocks malicious add-ons installed by 455K Firefox users

From the article: "Mozilla blocked malicious Firefox add-ons installed by roughly 455,000 users after discovering in early June that they were abusing the proxy API to block Firefox updates."

Source: https://www.bleepingcomputer.com/news/security/mozilla-blocks-malicious-add-ons-installed-by-455k-firefox-users/

Additional sources:
https://www.securityweek.com/mozilla-blocks-malicious-firefox-add-ons-abusing-proxy-api

https://cyberintelmag.com/malware-viruses/mozilla-blocks-malicious-add-ons-installed-by-455k-firefox-users/

https://www.zdnet.com/article/mozilla-firefox-cracks-down-on-malicious-add-ons-used-by-455000-users/

https://threatpost.com/mozilla-firefox-blocks-malicious-add-ons-installed-by-455k-users/175745/

https://cyberintelmag.com/malware-viruses/malicious-firefox-add-ons-interfered-how-browser-connects-to-the-internet/

Lazarus Attackers Turn to the IT Supply Chain

From the article: "Kaspersky researchers saw The North Korean state APT use a new variant of the BlindingCan RAT to breach a Latvian IT vendor and then a South Korean think tank."

Source: https://threatpost.com/lazarus-apt-it-supply-chain/175772/

Additional sources:
https://www.securityweek.com/kaspersky-north-korean-hackers-targeting-it-supply-chain

https://cyberintelmag.com/attacks-data-breaches/north-korean-lazarus-have-begun-to-target-the-it-supply-chain/

https://www.darkreading.com/threat-intelligence/north-korea-s-lazarus-group-turns-to-supply-chain-attacks

https://securityaffairs.co/wordpress/123831/apt/north-korea-lazarus-supply-chain.html

https://www.bleepingcomputer.com/news/security/north-korean-state-hackers-start-targeting-the-it-supply-chain/

DoJ & Europol Arrest 150 in Disruption of DarkNet Drug Operation

From the article: "Operation Dark HunTor targeted opioid traffickers on the DarkNet, leading to the seizure of weapons, drugs, and $31 million."

Source: https://www.darkreading.com/threat-intelligence/doj-europol-arrest-150-in-disruption-of-darknet-drug-operation

Additional sources:
https://www.cyberscoop.com/?p=59757

https://securityaffairs.co/wordpress/123818/cyber-crime/dark-huntor-operation.html

https://www.welivesecurity.com/2021/10/27/dark-huntor-150-arrested-31-million-seized-major-dark-web-bust/

https://www.bleepingcomputer.com/news/security/police-arrest-150-dark-web-vendors-of-illegal-drugs-and-guns/

https://www.securityweek.com/150-people-arrested-us-europe-darknet-drug-probe

CISA urges admins to patch critical Discourse code execution bug

From the article: "A critical Discourse remote code execution (RCE) vulnerability tracked as CVE-2021-41163 was fixed via an urgent update by the developer on Friday "

Source: https://www.bleepingcomputer.com/news/security/cisa-urges-admins-to-patch-critical-discourse-code-execution-bug/

Additional sources:
https://www.securityweek.com/cisa-raises-alarm-critical-vulnerability-discourse-forum-software

https://cyberintelmag.com/cloud-security/cisa-urges-admins-to-patch-critical-discourse-rce-bug/

https://securityaffairs.co/wordpress/123775/hacking/discourse-rce.html

https://threatpost.com/cisa-critical-rce-discourse/175705/

FBI Says Ranzy Locker Ransomware Encrypted 30 US Companies This Year

From the article: "The FBI said that the operators of the Ranzy Locker ransomware have compromised over 30 US companies."

Source: https://cyberintelmag.com/attacks-data-breaches/fbi-says-ranzy-locker-ransomware-encrypted-30-us-companies-this-year/

Additional sources:
https://www.bleepingcomputer.com/news/security/fbi-ranzy-locker-ransomware-hit-at-least-30-us-companies-this-year/

https://securityaffairs.co/wordpress/123801/cyber-crime/ranzy-locker-ransomware.html

https://www.securityweek.com/fbi-publishes-indicators-compromise-ranzy-locker-ransomware

https://www.tripwire.com/state-of-security/featured/fbi-warns-of-ranzy-locker-ransomware-threat-as-over-30-companies-hit/

New Gang Used Zero-day in Billing Software to Deploy Ransomware

From the article: "An unknown ransomware group is currently exploiting a SQL injection bug in BillQuick Web Suite to launch attacks on their target’s networks. The vulnerability is tracked as CVE-2021-42258."

Source: https://cyberintelmag.com/attacks-data-breaches/new-gang-used-zero-day-in-billing-software-to-deploy-ransomware/

Additional sources:
https://threatpost.com/billquick-billing-app-ransomware/175720/

https://www.bleepingcomputer.com/news/security/hackers-used-billing-software-zero-day-to-deploy-ransomware/

https://securityaffairs.co/wordpress/123783/cyber-crime/ransomware-gang-billquick-web-suite-bug.html

https://www.securityweek.com/billquick-billing-software-exploited-hack-us-engineering-company

Free decryptor released for Atom Silo and LockFile ransomware

From the article: "Avast has just released a decryption tool that will help AtomSilo and

LockFile ransomware victims recover some of their files for free, without having to pay a ransom."

Source: https://www.bleepingcomputer.com/news/security/free-decryptor-released-for-atom-silo-and-lockfile-ransomware/

Additional sources:
https://www.securityweek.com/free-decryption-tools-available-babuk-atomsilo-and-lockfile-ransomware

https://cyberintelmag.com/attacks-data-breaches/free-decryptor-for-the-malware-atom-silo-and-lockfile-has-been-released/

https://securityaffairs.co/wordpress/123854/malware/atomsilo-lockfile-ransomware-decryptor.html

https://www.bleepingcomputer.com/news/security/babuk-ransomware-decryptor-released-to-recover-files-for-free/

https://securityaffairs.co/wordpress/123844/malware/babuk-ransomware-decryptor.html

Millions of Android Users Infected in Subscription Fraud Campaign

From the article: "A massive fraud campaign was uncovered that is using over 150 Android apps. The apps have over 10 million downloads. The campaign is used to steal users' money by registering subscriptions for them without their knowledge."

Source: https://cyberintelmag.com/malware-viruses/millions-of-android-users-infected-in-subscription-fraud-campaign/

Additional sources:
https://www.bleepingcomputer.com/news/security/millions-of-android-users-targeted-in-subscription-fraud-campaign/

https://threatpost.com/android-scammed-sms-fraud-tik-tok/175739/

https://securityaffairs.co/wordpress/123795/malware/ultimasms-massive-fraud-campaign.html

https://cyberintelmag.com/malware-viruses/premium-sms-scam-apps-infect-over-10-million-android-users/

Adobe Patches Gaping Security Flaws in 14 Software Products

From the article: "Adobe on Tuesday released a slew of urgent patches with fixes for more than 90 documented vulnerabilities that expose Windows, macOS and Linux users to malicious hacker attacks."

Source: https://www.securityweek.com/adobe-patches-gaping-security-flaws-14-software-products

Additional sources:
https://www.zdnet.com/article/weeks-early-adobe-dumps-massive-security-patch-update/

https://go.theregister.com/feed/www.theregister.com/2021/10/26/adobe_october_extra_patches/

https://threatpost.com/critical-patches-adobe-security-bulletin/175825/

Emsisoft created a free decryptor for past victims of the BlackMatter ransomware

From the article: "Experts from cybersecurity firm Emsisoft announced the availability of a free decryptor for past victims of the BlackMatter ransomware."

Source: https://securityaffairs.co/wordpress/123736/security/blackmatter-decryptor-pat-victims.html

Additional sources:
https://www.theregister.com/2021/10/25/blackmatter_portal_emsisoft/

https://www.bleepingcomputer.com/news/security/blackmatter-ransomware-victims-quietly-helped-using-secret-decryptor/

https://cyberintelmag.com/attacks-data-breaches/emsisoft-quietly-decrypted-multiple-blackmatter-ransomware-victims/

Emergency Google Chrome update fixes zero-days used in attacks

From the article: "Google has released Chrome 95.0.4638.69 for Windows, Mac, and Linux to fix two zero-day vulnerabilities that attackers have actively exploited."

Source: https://www.bleepingcomputer.com/news/google/emergency-google-chrome-update-fixes-zero-days-used-in-attacks/

Additional sources:
https://securityaffairs.co/wordpress/123906/security/chrome-zero-day-flaws.html

https://www.securityweek.com/chrome-95-update-patches-exploited-zero-days-flaws-disclosed-tianfu-cup

https://cyberintelmag.com/cloud-security/latest-google-chrome-update-addresses-zero-day-vulnerabilities-exploited-in-cyberattacks/

REvil gang member identified living luxury lifestyle in Russia, says German media

From the article: "German news outlets claim to have identified a member of the infamous REvil ransomware gang – who reportedly lives the life of Riley off his ill-gotten gains."

Source:
https://www.theregister.com/2021/10/28/revil_member_identified_german_reports/

Additional sources:
https://www.bleepingcomputer.com/news/security/german-investigators-identify-revil-ransomware-gang-core-member/

https://www.bleepingcomputer.com/news/security/german-investigators-unmask-a-core-member-of-revil-ransomware-gang/

https://securityaffairs.co/wordpress/123867/cyber-crime/police-idenfied-revil-ransomware-member.html

Microsoft: Shrootless bug lets hackers install macOS rootkits

From the article: "Attackers could use a new macOS vulnerability discovered by

Microsoft to bypass System Integrity Protection (SIP) and perform arbitrary operations, elevate privileges to root, and install rootkits on vulnerable devices."

Source: https://www.bleepingcomputer.com/news/security/microsoft-shrootless-bug-lets-hackers-install-macos-rootkits/

Additional sources:
https://cyberintelmag.com/attacks-data-breaches/attackers-may-be-able-to-install-rootkit-on-macos-systems-due-to-a-new-shrootless-vulnerability/

https://securityaffairs.co/wordpress/123898/hacking/macos-shrootless-cve-2021-30892-flaw.html

https://www.theregister.com/2021/10/29/shrootless_macos_sip_bypass_microsoft/

https://www.securityweek.com/shrootless-macos-vulnerability-found-microsoft-allows-rootkit-installation

NSA and CISA share guidance on securing 5G cloud infrastructure

From the article: "CISA and the NSA shared guidance on securing cloud-native 5G networks from attacks seeking to compromise information or deny access by taking down cloud infrastructure."

Source: https://www.bleepingcomputer.com/news/security/nsa-and-cisa-share-guidance-on-securing-5g-cloud-infrastructure/

Additional sources:
https://www.darkreading.com/cloud/nsa-cisa-series-on-securing-5g-cloud-infrastructures

https://www.securityweek.com/nsa-cisa-release-5g-cloud-security-guidance

https://securityaffairs.co/wordpress/123910/reports/5g-networks-prevent-lateral-movement.html

MITRE, CISA Announce 2021 List of Most Common Hardware Weaknesses

From the article: "MITRE and the DHS’s Cybersecurity and Infrastructure Security

Agency (CISA) have announced the release of the “2021 Common Weakness Enumeration (CWE) Most Important Hardware Weaknesses” list."

Source: https://www.securityweek.com/mitre-cisa-announce-2021-list-most-common-hardware-weaknesses

Additional sources:
https://securityaffairs.co/wordpress/123948/security/2021-list-of-most-common-hardware-weaknesses.html

https://www.darkreading.com/vulnerabilities-threats/top-hardware-weaknesses-list-debuts

https://semiengineering.com/2021-cwe-most-important-hardware-weaknesses/

BillQuick Billing Software Exploited to Hack U.S. Engineering Company

Summary: SQL injection vulnerability in BillQuick software; lead to an exploitation through ransomware of an engineering company.

Source: https://www.securityweek.com/billquick-billing-software-exploited-hack-us-engineering-company

Semiconductors: The key to the future of electric vehicles

From the article: “"Ninety percent of the innovations in the automobile industry actually come from the electronics and the chips are the soul of the electronics," said Robert Li, vice president and general manager, PL driver and energy systems, NXP Semiconductors, one of the world's largest chip manufacturers.”

Source: https://newseu.cgtn.com/news/2021-10-20/Semiconductors-The-key-to-the-future-of-electric-vehicles-13Kivj0gEfu/index.html

A Look Inside Modern Design Principles for Secure Boot in CPU Hardware

From the article: “Secure boot capabilities have been around for almost two decades in commodity parts. These capabilities are meant to provide users or owners with confidence that a device has booted up securely and with approved firmware authorized by the original manufacturer."

Source:
https://www.networkcomputing.com/network-security/look-inside-modern-design-principles-secure-boot-cpu-hardware

Northrop Grumman establishes new microelectronics packaging facility

From the article: "Northrop Grumman has continued to invest in the future of defense microelectronics systems takes another leap forward with the creation of its "Micro-Line" (u-Line) in Apopka. The company's new u-Line establishes a wafer post-processing and test source tailored for defense applications."

Source:
https://www.spacedaily.com/reports/Northrop_Grumman_establishes_new_microelectronics_packaging_facility_999.html

Bosch to invest more than 400 mln eur in chip production

From the article: "German technology group Robert Bosch (ROBG.UL) has earmarked more than 400 million euros ($467 million) for investments in microchip production in Germany and Malaysia next year to ease a global shortage."

Source: https://www.reuters.com/technology/bosch-invest-more-than-400-mln-eur-chip-production-2021-10-29/

Intel teams with Google Cloud to develop new class of data center chip

From the article: "Intel Corp (INTC.O) and Alphabet Inc's (GOOGL.O) Google Cloud on Wednesday said they have worked together to create a new category of chip that Intel hopes will become a major seller in the booming cloud computing market."

Source: https://www.reuters.com/technology/intel-teams-with-google-cloud-develop-new-class-data-center-chip-2021-10-27/

TSMC promises performance and power efficiency gains with its new 5nm 'N4P' process

From the article: “On Tuesday, Taiwan Semiconductor Manufacturing Company (TSMC) announced its N4P process. The 5nm enhancement should provide more choices for customers alongside its N5, N4, and N3 processes.”

Source: https://www.techspot.com/news/91946-tsmc-announces-new-5nm-n4p-process.html

Microsoft Warns About New Version of UpdateAgent Targeting Macs

Summary: MSTIC has discovered a new version of UpdateAgent targeting Mac devices.

Source: https://cyberintelmag.com/malware-viruses/microsoft-warns-about-new-version-of-updateagent-targeting-macs/

Researchers Describe New Attack That Spoofs Browser’s Digital Fingerprints

Summary: Gummy Browsers method allows a malicious website to harvest browser -fingerprint information then coordinate with another device to replay the fingerprint information to a legitimate site.

Source: https://cyberintelmag.com/attacks-data-breaches/researchers-describe-new-attack-that-spoofs-browsers-digital-fingerprints/

Release of SCAIFE System Version 2.0.0 Provides Support for Continuous-Integration (CI) Systems

Summary: SCAIFE is an automated static code analyzer system. New version now works with conitnuous integration builds. The tools also make use of AI to help with static code analysis.

Source: https://insights.sei.cmu.edu/blog/release-of-scaife-system-version-200-provides-support-for-continuous-integration-ci-systems/

Our ICS-Themed Pwn2Own Contest Returns to Miami in 2022

Summary: ICS based pwn2own contest in Miami at the S4x22 event.

Source: https://www.thezdi.com/blog/2021/10/22/our-ics-themed-pwn2own-contest-returns-to-miami-in-2022

Extracting type information from Go binaries

Summary: Tutorial on extracting type information from binaries based on the Go language.

Source: https://securelist.com/extracting-type-information-from-go-binaries/104715/

NIST's new devsecops guidance to aid transition to cloud-native apps

Summary: NIST draft document SP800-204C Implementation of DevSecOps for a Microservices-based Application with Service Mesh released in September; this document shows the path for implementing devsecops in a cloud environment.

Source: https://www.csoonline.com/article/3637120/nists-new-devsecops-guidance-to-aid-transition-to-cloud-native-apps.html

Department of Energy Announces $10M in Funding to Cooperative and Municipal Utilities to Secure the Energy Sector's Industrial Control Systems

Summary: US DOE CESER announces $10 million funding for cybersecurity to municiple and cooperative energy infrastructure organizations

Source: https://www.energy.gov/ceser/articles/department-energy-announces-10m-funding-cooperative-and-municipal-utilities-secure

'Cyber event' knocks dairy giant Schreiber Foods offline amid industry ransomware outbreak

Summary: A cyber attack aimed at Schreiber Foods brought plants and distribution for the company down.

Source: https://www.cyberscoop.com/?p=59797

FBI Publishes Indicators of Compromise for Ranzy Locker Ransomware

Summary: FBI issues IOCs for Ranzy Locker ransomware. Ransomware targets business in US, IT sector and usually starts with an RDP brute force attack.

Source: https://www.securityweek.com/fbi-publishes-indicators-compromise-ranzy-locker-ransomware

Dragos Becomes First Industrial Cybersecurity Unicorn After Raising $200 Million

Summary: Dragos becomes a 'unicorn' class startup; first in the control system security space.

Source: https://www.securityweek.com/dragos-becomes-first-industrial-cybersecurity-unicorn-after-raising-200-million

Microsoft finds new macOS vulnerability, Shrootless, that could bypass System Integrity Protection

Summary: Microsoft performed a coordinated vulnerability disclosure to Apple about a vulnerability in MacOS

Source: https://www.microsoft.com/security/blog/2021/10/28/microsoft-finds-new-macos-vulnerability-shrootless-that-could-bypass-system-integrity-protection/

NSA-CISA Series on Securing 5G Cloud Infrastructures

Summary: NSA-CISA releases guidance on security 5G cloud infrastructures

Source: https://us-cert.cisa.gov/ncas/current-activity/2021/10/28/nsa-cisa-series-securing-5g-cloud-infrastructures

All Windows versions impacted by new LPE zero-day vulnerability

Summary: To successfully abuse this vulnerability (LPE = Local Privilege Escalation); the attacker needs local access and username/password information of another user on the system

Source: https://www.bleepingcomputer.com/news/security/all-windows-versions-impacted-by-new-lpe-zero-day-vulnerability/

I'm Not a Pilot, but I Just Flew a Helicopter Over California

Summary: NYTimes article on AI and the new flight technologies to open the world of flying

Source: https://catless.ncl.ac.uk/Risks/32/91/#subj11.1

Businesses Are Exposed More as Non-Business IoT Devices on Corporate Networks Grow

From the article: "The adoption of the Internet of Things has become a significant business enabler. According to Vicky Ray, lead researcher, Unit 42 at Palo Alto Networks, it offers new security concerns that can only be handled if employees and employers take responsibility for network security. Remote employees should be cautious of home equipment that might connect to business networks through their home router. To protect remote employees and the organization's most important assets, businesses must better monitor threats and network access and provide a level of segmentation."

Source: https://cyberintelmag.com/iot/businesses-are-exposed-more-as-non-business-iot-devices-on-corporate-networks-grow/

Avoiding the costly ESU cycle: Lessons learned from Windows 7 end-of-life

From the article: "A unique challenge facing organizations with the end-of-life date for Windows 10 and the move to Windows 11 is the new OS's exclusive support for 64-bit edition apps. Up until now, it's been easy for businesses to ensure compatibility for older apps because Windows 10 came also in a 32-bit version, but this is all set to change. On top of this, Windows 10 features are already being deprecated in preparation for Windows 11's introduction. The removal of small features over the coming years may create a big problem if an organization's app relies on them. The time to act is now, and organizations need the supporting expertise and solutions to make it happen."

Source: https://www.helpnetsecurity.com/2021/11/01/end-of-life-windows-7/

The joy of VEX, part I

Summary: Overview of the VEX document format, a companion to the SBOM.

Source: http://tomalrichblog.blogspot.com/2021/10/the-joy-of-vex-part-i.html

Cybercriminals Take Aim at Connected Car Infrastructure

From the article: "With automobiles becoming increasingly connected, a variety of attacks are emerging: Car thieves abuse keyless entry systems, hackers find new ways to exploit vehicle components, and fraud targets auto financing, automotive cybersecurity experts said in interviews this week. In September, for example, New York City police raided a car-theft ring that reportedly stole cars using cloned key fobs based on security codes bought online and encoded into a device by a local locksmith. They also used an aftermarket scanning tool, typically used by mechanics, to reprogram targeted cars' ignitions to make them think all the keys had been lost."

Source: https://www.darkreading.com/attacks-breaches/cybercriminals-take-aim-at-connected-car-infrastructure

CISA starts identifying targets most necessary to protect from hacking

Summary: CISA has started to map out critical infrastructure targets and prioritize what needs to be protected by cybersecurity

Source: https://www.cyberscoop.com/sici-easterly-katko-psies-csis-cisa/

Comments to the US Secretary of Energy's Advisory Board on lack of process sensor cyber security

Summary: Joe Weiss summary of his comments to the US Secretary of Energy's Advisory Board on process sensor cybersecurity

Source: https://www.controlglobal.com/blogs/unfettered/comments-to-the-us-secretary-of-energys-advisory-board-on-lack-of-process-sensor-cyber-security/

Hive ransomware now encrypts Linux and FreeBSD systems

From the article: "The Hive ransomware gang now also encrypts Linux and FreeBSD using new malware variants specifically developed to target these platforms. However, as Slovak internet security firm ESET discovered, Hive's new encryptors are still in development and still lack functionality. The Linux variant also proved to be quite buggy during ESET's analysis, with the encryption completely failing when the malware was executed with an explicit path."

Source: https://www.bleepingcomputer.com/news/security/hive-ransomware-now-encrypts-linux-and-freebsd-systems/

TTC investigating after hit by ransomware attack

From the article: "The attack has crippled the TTC's Vision System, which is used to communicate with vehicle operators. "We do have radio backup, so there's no issue communicating with the operators," Green said. Hackers also took down the 'Next Vehicle Information System' on platform screens, trip-planning apps, the TTC website, and the online Wheel-Trans online booking portal. The TTC's internal email service was also affected. "I'm talking to you on my personal phone because we don't have network systems here or network service here at the TTC office. So, I don't have email. I don't have internet service. So that's the kind of thing that's being impacted right now," Stuart said."

Source: https://www.cp24.com/news/ttc-investigating-after-hit-by-ransomware-attack-1.5644928

What's New in the OWASP Top 10 2021?

From the article: "...brand new category in the number four position: insecure design. This focuses on risks related to design flaws. Van der Stock is a former app designer himself. As such, he says this category isn't a catch-all for anything that doesn't make sense anywhere else. The bucket, he said, represents any control that is missing, ineffective or by-passable in code. "

Source: https://securityintelligence.com/articles/whats-new-owasp-top-10-2021/

Infrastructure Security Month | CISA

Summary: CISA kicks off Infrastructure Security Month:
Week 1: Shared risk means building shared responsibility
Week 2: Soft Target Security
Week 3: Resilience in Critical Infrastructure
Week 4: Secure our Elections

Source: https://www.cisa.gov/infrastructure-security-month

China Tightens Control Over Company Data With Transfer Rules

Summary: in particular this rule deals with transfer of personal information.

Source: https://www.securityweek.com/china-tightens-control-over-company-data-transfer-rules

Q3 2021 Cyber Attacks Statistics

Summary: HACKMAGGEDON's Q3 2021 attack statistics

Source: https://www.hackmageddon.com/2021/11/02/q3-2021-cyber-attacks-statistics/

How to hack a phone: 7 common attack methods explained

Summary: Summary of ways to hack a smart phone

Source: https://www.csoonline.com/article/2112407/identity-access-3-simple-steps-to-hack-a-smartphone-includes-video

Energy industry hit by surge in mobile phishing threats

Summary: Mobile phishing targeting energy industry workers have hit a high in 2021. This attack vector leverages the mobile device path along with a human in the loop.

Source: https://betanews.com/2021/11/02/energy-industry-surge-mobile-phishing/

Security patch 'all about the optics,' government adviser says when told installing it didn't make sense - National Post

Summary: When patching takes a political tone. Example of a Microsoft Exchange patch in the Canadian government where one agency argued it made no sense due to their network being disconnected, however, the 'optics' of the patch being deployed trumped the effectiveness.

Source: https://nationalpost.com/news/politics/security-patch-all-about-the-optics-government-adviser-says-when-told-installing-it-didnt-make-sense

Cybercriminals flog access to international shipping, logistics giants

From the article: "According to the cybersecurity firm, this actor had previously given Conti access to a botnet including a virtual network computing (VNC) function, allowing them "to download and execute a Cobalt Strike beacon on infected machines, so group members in charge of breaching computer networks received access directly via a Cobalt Strike beacon session." A posting published in September by an IAB linked to the FiveHands ransomware group offered access to "hundreds" of companies, including a logistics company in the United Kingdom, whereas in other postings on cybercriminal forums, access to a shipping firm in Bangladesh -- secured through a PulseSecure VPN security flaw -- local admin rights in a US freight organization, and a pack of credentials including account access for a logistics company in Malaysia were also on offer. "

Source: https://www.zdnet.com/article/cybercriminals-flog-access-to-international-shipping-logistics-giants-in-the-underground/#ftag=RSSbaffb68

Police arrest criminals behind Norsk Hydro ransomware attack

From the article: "The Europol has announced the arrest of 12 individuals who are believed to be linked to ransomware attacks against 1,800 victims in 71 countries."

Source: https://www.bleepingcomputer.com/news/security/police-arrest-criminals-behind-norsk-hydro-ransomware-attack/

Additional sources:
https://securityaffairs.co/wordpress/123915/cyber-crime/individuals-1800-ransomware-attacks.html?

https://www.securityweek.com/12-people-arrested-over-ransomware-attacks-critical-infrastructure

https://thehackernews.com/2021/10/police-arrest-suspected-ransomware.html

Spammers use Squirrelwaffle malware to drop Cobalt Strike

From the article: "A new malware threat named Squirrelwaffle has emerged in the wild, supporting actors with an initial foothold and a way to drop malware onto compromised systems and networks."

Source: https://www.bleepingcomputer.com/news/security/spammers-use-squirrelwaffle-malware-to-drop-cobalt-strike/

Additional sources:
https://threatpost.com/squirrelwaffle-loader-malspams-packing-qakbot-cobalt-strike/175775/

https://cyberintelmag.com/malware-viruses/squirrelwaffle-virus-used-by-spammers-to-distribute-cobalt-strike/

https://blog.talosintelligence.com/2021/10/squirrelwaffle-emerges.html

CISA selects Kim Wyman, GOP official who criticized false election fraud claims, as election security leader

From the article: "Kim Wyman, Washington's secretary of state since 2013, will take the job of senior election security lead at CISA, the Department of Homeland Security's primary cybersecurity arm."

Source: https://www.cyberscoop.com/?p=59768

Additional sources:
https://www.darkreading.com/vulnerabilities-threats/cisa-announces-appointment-of-washington-secretary-of-state-kim-wyman-as-senior-election-security-lead

https://www.securityweek.com/washington-secretary-state-appointed-cisa

Expert managed to crack 70% of a 5,000 WiFi network sample in Tel Aviv

From the article: "A researcher from the security firm CyberArk has managed to crack 70% of Tel Aviv's Wifi Networks starting from a sample of 5,000 gathered WiFi."

Source: https://securityaffairs.co/wordpress/123810/hacking/cracking-wifi-at-scale.html

Additional sources:
https://www.bleepingcomputer.com/news/security/researcher-cracked-70-percent-of-wifi-networks-sampled-in-tel-aviv/

https://threatpost.com/war-driving-wi-fi-password-cracking/175817/

To Infect Visitors, Ransomware Gangs Using SEO Poisoning

From the article: "Researchers have discovered two operations that leverage SEO poisoning to deliver payloads to targets."

Source: https://cyberintelmag.com/attacks-data-breaches/to-infect-visitors-ransomware-gangs-using-seo-poisoning/

Additional sources:
https://www.bleepingcomputer.com/news/security/ransomware-gangs-use-seo-poisoning-to-infect-visitors/

https://www.darkreading.com/attacks-breaches/seo-poisoning-used-to-distribute-ransomware

US bans China Telecom Americas over national security risks

From the article: "The Federal Communications Commission (FCC) has revoked China Telecom Americas' license to provide telecommunication services within the United States."

Link to FCC documents: https://www.fcc.gov/document/fcc-revokes-china-telecom-americas-telecom-services-authority

Source: https://www.bleepingcomputer.com/news/security/us-bans-china-telecom-americas-over-national-security-risks/

Additional sources:
https://www.securityweek.com/us-bans-china-telecom-over-national-security-concerns

https://www.theregister.com/2021/10/27/china_telecom_booted_out_of/

Brutal WordPress plugin bug allows subscribers to wipe sites

From the article: "A high severity security flaw found in a WordPress plugin with more than 8,000 active installs can let authenticated attackers reset and wipe vulnerable websites."

Source: https://www.bleepingcomputer.com/news/security/brutal-wordpress-plugin-bug-allows-subscribers-to-wipe-sites/

Additional sources:
https://threatpost.com/wordpress-plugin-bug-wipe-sites/175826/

https://cyberintelmag.com/cloud-security/subscribers-can-erase-sites-due-to-a-severe-wordpress-plugin-vulnerability/

WordPress Plugin Flaw Affects 1 Million Sites And Allows For Malicious Redirection

From the article: "A high-severity issue in the OptinMonster plugin permits unauthorized API access and sensitive information exposure on around a million WordPress sites."

Source: https://cyberintelmag.com/cloud-security/wordpress-plugin-flaw-affects-1-million-sites-and-allows-for-malicious-redirection/

Additional sources:
https://www.bleepingcomputer.com/news/security/wordpress-plugin-bug-impacts-1m-sites-allows-malicious-redirects/

https://securityaffairs.co/wordpress/123886/hacking/wordpress-optinmonster-plugin-flaws.html

Apple Patches 22 Security Flaws Haunting iPhones

From the article: "Apple has released another IOS 15 update with patches for 22 serious security defects in a wide range of iPhone and iPad software components."

Source: https://www.securityweek.com/apple-patches-22-security-flaws-haunting-iphones

Additional sources:
https://threatpost.com/apple-patches-ios-bugs/175803/

https://cyberintelmag.com/attacks-data-breaches/apple-fixes-critical-ios-bugs-one-is-targeted/

New AbstractEmu malware roots Android devices, evades detection

From the article: "New Android malware can root infected devices to take complete control and silently tweak system settings, as well as evade detection using code abstraction and anti-emulation checks."

Source: https://www.bleepingcomputer.com/news/security/new-abstractemu-malware-roots-android-devices-evades-detection/

Additional sources:
https://securityaffairs.co/wordpress/123873/malware/abstractemu-android-malware.html

Cleanup on aisle C: Tesco app back online after attack led to shopping app outages

From the article: "The UK's largest retailer, supermarket titan Tesco, has restored its online operations after an attack hack left its customers unable to order, amend, or cancel deliveries for two days."

Source: https://www.theregister.com/2021/10/25/tesco_outage/

Additional sources:
https://cyberintelmag.com/attacks-data-breaches/tescos-website-and-app-went-offline-after-suspected-cyberattack/

NYT Journalist's iPhone infected twice with NSO Group'sPegasus spyware

From the article: "Threat actors infected the iPhone of New York Times journalist Ben Hubbard with NSO Group's Pegasus spyware between June 2018 to June 2021."

Source: https://securityaffairs.co/wordpress/123747/hacking/nyt-journalist-pegasus-spyware.html

Additional sources:
https://www.schneier.com/blog/archives/2021/10/new-york-times-journalist-hacked-with-nso-spyware.html

Facebook Sues Ukrainian for Scraping, Selling Data of 178 Million Users

From the article: "Facebook last week filed a lawsuit against a Ukrainian national who allegedly scraped the information of 178 million of its users and then sold the obtained information on hacker forums."

Source: https://www.securityweek.com/facebook-sues-ukrainian-scraping-selling-data-178-million-users

Additional sources:
https://go.theregister.com/feed/www.theregister.com/2021/10/25/facebook_sues_man_for_scraping/

India's Top Court Orders Probe Into Pegasus Snooping

From the article: "India's Supreme Court on Wednesday ordered an independent investigation into the alleged government use of Pegasus spyware on journalists, opposition politicians and activists with the chief justice calling the implications "Orwellian"."

Source: https://www.securityweek.com/indias-top-court-orders-probe-pegasus-snooping

Additional sources:
https://www.theregister.com/2021/10/29/india_nso_pegasus_probe/

TodayZoo phishing kit borrows the code from other kits

From the article: "Microsoft uncovered an extensive series of credential phishing campaigns that employed a custom phishing kit tracked as TodayZoo."

Source: https://securityaffairs.co/wordpress/123729/cyber-crime/todayzoo-phishing-kit.html

Additional sources:
https://cyberintelmag.com/malware-viruses/microsoft-warns-of-custom-todayzoo-phishing-kit-used-for-credential-stealing/

Kansas Man Admits Hacking Public Water Facility

From the article: "Roughly seven months after being indicted for his actions, a Kansas man admitted in court to tampering with the systems at the Post Rock Rural Water District."

Source: https://www.securityweek.com/kansas-man-admits-hacking-public-water-facility

Additional sources:
https://securityaffairs.co/wordpress/123791/cyber-crime/post-rock-rural-water-district-hack.html

FBI Raids Chinese Point-of-Sale Giant PAX Technology

From the article: "U.S. federal investigators today raided the Florida offices of PAX Technology, a Chinese provider of point-of-sale devices used by millions of businesses and retailers globally."

Source: https://krebsonsecurity.com/2021/10/fbi-raids-chinese-point-of-sale-giant-pax-technology/

Additional sources:
https://go.theregister.com/feed/www.theregister.com/2021/10/27/pax_technology_warehouse_raid/

Squid Game-themed App Was Spreading Joker On Play Store

From the article: "The popularity of Squid Game has also caught up with the hackers. Security researchers detected that the Squid Game wallpapers app was being used to spread mobile malware."

Source: https://cyberintelmag.com/malware-viruses/squid-game-themed-app-was-spreading-joker-on-play-store/

Additional sources:
https://www.darkreading.com/vulnerabilities-threats/ready-to-play-squid-game-becomes-an-attractive-lure-to-spread-cyberthreats

Massachusetts Health Network Hacked; Patient Info Exposed

From the article: "A Worcester, Mass. health care network says someone hacked into its employee email system, potentially exposing the personal information of thousands of patients."

Source: https://www.securityweek.com/massachusetts-health-network-hacked-patient-info-exposed

Additional sources:
https://securityaffairs.co/wordpress/123970/data-breach/umass-memorial-health-cyberattack.html

Scammers are emailing waves of unsolicited QR codes, aiming to steal Microsoft users' passwords

From the article: "Email fraudsters are seizing on the attention around the quick response codes that have become more common in restaurants and stories, leveraging QR codes try to steal users' Microsoft credentials and other data."

Source: https://www.cyberscoop.com/?p=59767

Additional sources:
https://www.darkreading.com/attacks-breaches/qr-codes-help-attackers-sneak-emails-past-security-controls

Malicious NPM libraries install ransomware, password stealer

From the article: "Malicious NPM packages pretending to be Roblox libraries are delivering ransomware and password-stealing trojans on unsuspecting users."

Source: https://www.bleepingcomputer.com/news/security/malicious-npm-libraries-install-ransomware-password-stealer/

Additional sources:
https://cyberintelmag.com/malware-viruses/password-stealer-and-ransomware-getting-installed-via-malicious-npm-libraries/

US charges alleged extortionist, HeheStreams operator with demanding $150K from MLB

From the article: "Attorneys from the Southern District of New York charged Joshua Streit with running HeheStreams.com, a website that allowed users to stream games from the MLB, National Hockey League, National Basketball Association and the National Football League for a fee, according to a complaint."

Source: https://www.cyberscoop.com/us-charges-mlb-hehestreams-joshua-streit/

Additional sources:
https://www.bleepingcomputer.com/news/security/doj-pirated-sports-streamer-hacked-accounts-extorted-mlb/

'Cyber event' knocks dairy giant Schreiber Foods offline amid industry ransomware outbreak

From the article: "A “cyber event” knocked plants and distribution centers offline at Schreiber Foods, a multibillion-dollar dairy company, a spokesperson told CyberScoop Wednesday."

Source: https://www.cyberscoop.com/?p=59797

Additional sources:
https://cyberintelmag.com/attacks-data-breaches/after-a-ransomware-cyberattack-shut-down-milk-factories-schreiber-foods-is-back-to-normal/

Due To a Network Issue, Users Can't Enroll Google Chromebooks, Compromising Security

From the article: "Recently, Google has been looking into consumers having trouble registering their Chromebooks due to a network fault, thus compromising user security."

Source: https://cyberintelmag.com/attacks-data-breaches/due-to-a-network-issue-google-chromebooks-are-unable-to-enroll/

Additional sources:
https://www.bleepingcomputer.com/news/security/google-chromebooks-failing-to-enroll-due-to-network-issue/

Threat actors offer for sale data for 50 millions of Moscow drivers

From the article: "Threat actors are offering for sale a database containing 50 million records belonging to Moscow drivers on a hacking forum for $800."

Source: https://securityaffairs.co/wordpress/123711/data-breach/moscow-drivers-data-leak.html

NATO releases its first strategy for Artificial Intelligence

From the article: "This week, NATO Defence Ministers released the first-ever strategy for Artificial Intelligence (AI) that encourages the use of AI in a responsible manner."

Source: https://securityaffairs.co/wordpress/123715/security/nato-strategy-artificial-intelligence.html

Microsoft 365 will get support for custom ARC configurations

From the article: "Microsoft is working on adding custom Authenticated Received Chain (ARC) configuration support to Microsoft Defender for Office 365."

Source: https://www.bleepingcomputer.com/news/microsoft/microsoft-365-will-get-support-for-custom-arc-configurations/

Scaling Bump Pitches In Advanced Packaging

From the article: "Interconnects for advanced packaging are at a crossroads as an assortment of new package types are pushing further into the mainstream, with some vendors opting to extend the traditional bump approaches while others roll out new ones to replace them."

Source: https://semiengineering.com/scaling-bump-pitches-in-advanced-packaging/

How deepfakes enhance social engineering and authentication threats, and what to do about it

From the article: "Deepfake technology is an escalating cybersecurity threat to organizations. Cybercriminals are investing in AI and machine learning to create synthetic or manipulated digital content (including images, video, audio and text) for use in cyberattacks and fraud."

Source: https://www.csoonline.com/article/3636992/how-deepfakes-enhance-social-engineering-and-authentication-threats-and-what-to-do-about-it.html

HIV Scotland fined £10,000 for BCC email blunder identifying names of virus-carriers' patient-advocates

From the article: "The United Kingdom's data watchdog is calling on organisations to review their "bulk email practices" after a BCC blunder by HIV Scotland incurred a £10,000 fine for breaking data protection regulations.…"

Source: https://www.theregister.com/2021/10/25/hiv_scotland_email_fail/

Researcher Earns $2 Million for Critical Vulnerability in Polygon

From the article: "Security researcher Gerhard Wagner earned a $2 million bug bounty reward for a critical vulnerability in Polygon's Plasma Bridge that could have allowed a malicious user to submit the same withdrawal transaction 224 times, with different exit IDs."

Source: https://www.securityweek.com/researcher-earns-2-million-critical-vulnerability-polygon

The Future of Farming: LoRaWAN®-powered Cattle Tracking Solutions

From the article: "Smart agriculture technologies assist farmers in improving all areas of agricultural productivity."

Source: https://www.iotforall.com/?p=124820

Cybersecurity First: Becoming GOAT

From the article: "As we close off Cybersecurity Awareness Month, let us examine how we can become the cyber GOAT: 'greatest of all time'. Sure, there will be plenty this week on cybersecurity training, making security a priority, more investments into products and processes and all that fun stuff."

Source: https://securityintelligence.com/articles/cybersecurity-first-becoming-goat/

Red TIM Research found two rare flaws in Ericsson OSS-RC component

From the article: "The Red Team Research (RTR), the bug's research division from Italian Telecommunication firm TIM, found 2 new vulnerabilities affecting the Ericsson OSS-RC."

Source: https://securityaffairs.co/wordpress/123764/security/ericsson-oss-rc-flaws.html

Russian spies compromised 14 tech providers, aiming to 'piggyback' on customer

access, Microsoft says

From the article: "Suspected Russian spies who exploited a federal contractor to breach nine U.S. government agencies last year have continued targeting technology supply chains, aiming to compromise 140 technology service providers in recent months, according to Microsoft."

Source: https://www.cyberscoop.com/?p=59737

How We Can Narrow the Talent Shortage in Cybersecurity

From the article: "Filling crucial roles in cybersecurity and addressing the talent shortage requires rethinking who qualifies as a "cybersecurity professional" and rewriting traditional job descriptions."

Source: https://www.darkreading.com/careers-and-people/how-we-can-narrow-the-talent-shortage-in-cybersecurity

6 Questions to Ask to Drive and Realize IoT Success

From the article: "Getting to the end of a complicated IoT project isn't about guesswork, nor is it simply about grinding it out. Here are six questions to ask to drive IoT success."

Source: https://www.iotforall.com/?p=131763

MWC Los Angeles 2021, in Partnership with CTIA, Announces Event Highlights

From the article: "The MWC Los Angeles conference program will include compelling keynotes from CEOs, thought leaders, and world-class exhibitors from the mobile ecosystem and adjacent industry sectors."

Source: https://www.iotforall.com/press-releases/https-www-gsma-com-newsroom-press-release-mwc-los-angeles-2021-in-partnership-with-ctia-announces-event-highlights

It's Windows XP's 20th birthday and way too many still use it

From the article: "Today is the 20th anniversary of Windows XP, and although the operating system reached the end of support in 2014, way too many people continue to use the insecure version of Windows."

Source: https://www.bleepingcomputer.com/news/microsoft/its-windows-xps-20th-birthday-and-way-too-many-still-use-it/

A Journey in Organizational Resilience: Privacy

From the article: "Privacy concerns may not be the first issue that comes to mind when building an enterprise cyber resilience plan."

Source: https://securityintelligence.com/articles/journey-organizational-resilience-privacy/

Microsoft Defender ATP adds live response for Linux and macOS

From the article: "Microsoft has announced the addition of new live macOS and Linux response capabilities to Defender for Endpoint, , the enterprise version of Redmond's Windows 10 Defender antivirus."

Source: https://www.bleepingcomputer.com/news/microsoft/microsoft-defender-atp-adds-live-response-for-linux-and-macos/

South Korean telco KT suffers nationwide outage after routing error

From the article: "The second-largest telecommunications provider in South Korea, KT Corporation, has suffered a nationwide outage today, leaving all its 16.5 million customers without internet connectivity and telephony services for about 40 minutes."

Source: https://www.bleepingcomputer.com/news/technology/south-korean-telco-kt-suffers-nationwide-outage-after-routing-error/

Conti Ransom Gang Starts Selling Access to Victims

From the article: "The Conti ransomware affiliate program appears to have altered its business plan recently."

Source: https://krebsonsecurity.com/2021/10/conti-ransom-gang-starts-selling-access-to-victims/

Who's In Your Wallet? Exploring Mobile Wallet Security

From the article: "Security flaws in contactless payments for transportation systems could lead to fraud for stolen devices, researchers find."

Source: https://www.darkreading.com/mobile/who-s-in-your-wallet-exploring-mobile-wallet-security

Changing Approaches to Preventing Ransomware Attacks

From the article: "Conducting scaled and cost-effective attack surface and digital threat monitoring gives organizations of all sizes the best chance of identifying and defeating their adversaries."

Source: https://www.securityweek.com/changing-approaches-preventing-ransomware-attacks

Groove Calls for Cyberattacks on US as REvil Payback

From the article: "The bold move signals a looming clash between Russian ransomware groups and the U.S."

Industrial Goods & Services Tops Ransomware Targets in 2021

From the article: "While the industrial goods and services sector saw a decline in attacks during the third quarter, it remains the most targeted sector for ransomware this year."

Source: https://www.darkreading.com/attacks-breaches/industrial-goods-services-tops-ransomware-targets-in-2021

5 Cybersecurity Considerations for the Auto Industry

From the article: "Technology has become an essential part of daily life. From the way we get around to the things we buy, computers are at the forefront of change."

Source: https://www.tripwire.com/state-of-security/security-data-protection/iot/5-cybersecurity-considerations-for-the-auto-industry/

From Device to Dashboard with Cellular IoT

From the article: "In this webinar, folks from Blues Wireless and Ubidots guide IoT developers through a typical journey from device to cloud using the cellular capabilities of Notecard and the data visualization platform provided by Ubidots."

Source: https://www.iotforall.com/webinar/from-device-to-dashboard-with-cellular-iot

Defending Assets You Don’t Know About Against Cyberattacks

From the article: "No security defense is perfect, and shadow IT means no company can inventory every single asset that it has. David “moose” Wolpoff, CTO at Randori, discusses strategies for core asset protection given this reality."

Source: https://threatpost.com/defending-unknown-assets-cyberattacks/175730/

If you're using this hijacked NPM library anywhere in your software stack, read this

From the article: "US govt issues alert over JS package downloaded 8m times a week – plus more news from world of infosec"

Source: https://www.theregister.com/2021/10/25/in_brief_security/

Additional sources:
https://www.bleepingcomputer.com/news/security/popular-npm-library-hijacked-to-install-password-stealers-miners/

Jumio Launches End-to-end Orchestration for its KYX Platform

From the article: "Platform combines digital identity proofing, compliance verification and anti-money laundering checks."

Source: https://www.darkreading.com/operations/jumio-launches-end-to-end-orchestration-for-its-kyx-platform

OpenText Strengthens Ransomware Resilience

From the article: "New detection and alert functions within Carbonite Server increase data protection against ransomware."

Source: https://www.darkreading.com/attacks-breaches/opentext-strengthens-ransomware-resilience

GCHQ director outlines plan to 'go after' links between ransomware crims and state actors

From the article: "Sir Jeremy Fleming paints picture of a cultural battle over the internet, AI and the soul of future technology."

Source: https://www.theregister.com/2021/10/26/gchq_ransomware_plan/

Power/Performance Bits: Oct. 26

From the article: "Researchers at Pennsylvania State University propose a way to print biodegradable circuits on irregular, complex shapes."

Source: https://semiengineering.com/power-performance-bits-oct-26/

Strategies For Meeting Stringent Standards For Automotive ICs

From the article: "It may surprise you, but when it comes to chips in electronic braking systems, airbag control units, and more, automotive manufacturers are still using 10-year-old technology — and with good reason."

Source: https://semiengineering.com/strategies-for-meeting-stringent-standards-for-automotive-ics/

Manufacturing Bits: Oct. 26

From the article: "At the upcoming IEEE International Electron Devices Meeting (IEDM) in San Francisco, a slew of entities will present papers on the latest technologies in R&D."

Source: https://semiengineering.com/manufacturing-bits-oct-26/

Schools put the brakes on facial recognition scheme for kids buying lunch

From the article: "UK regulators swooped in before the program gained full momentum."

Source: https://www.zdnet.com/article/schools-put-the-brakes-on-facial-recognition-scheme-for-kids-buying-lunch/

10 essential skills and traits of ethical hackers

From the article: "What if you could spend your days trying to gain access to other people's networks and computer systems—and not get in trouble for it?"

Source: https://www.csoonline.com/article/3637732/10-essential-skills-and-traits-of-ethical-hackers.html

US State Department Sets Up Cyber Bureau, Envoy Amid Hacking Alarm

From the article: "US Secretary of State Antony Blinken announced Monday that the State Department will establish a new bureau and envoy to handle cyber policy, revamping amid alarm over rising hacking attacks."

Source: https://www.securityweek.com/us-state-department-sets-cyber-bureau-envoy-amid-hacking-alarm

DDoSers take weekend off only to resume campaign against UK's Voipfone on Monday

From the article: "It never rains but it pours. Internet telephone service provider Voipfone, currently battling a "major outage" across all voice services, has admitted to being hit by an "extortion-based DDoS attack from overseas criminals" that knocked it offline last week.…"

Source:
https://go.theregister.com/feed/www.theregister.com/2021/10/26/voipfone_outage/

Blues Wireless Introduces Swan, A Companion to its Cellular Notecard, to Accelerate IoT Development Journey

From the article: "Swan from Blues Wireless is a low-cost, feather-compatible board that delivers unprecedented capabilities."

Source: https://www.iotforall.com/?post_type=press-releases&p=133991

Pratexo Wins Edge Startup of the Year at Edge Computing World 2021

From the article: "Pratexo Inc., the plug and play edge computing platform-as-a-service, announced its award as the Startup of the Year, as selected by a panel of independent judges at Edge Computing World 2021."

Source: https://www.iotforall.com/?post_type=press-releases&p=134424

Nearly all US execs have experienced a cybersecurity threat, but some say there's still no plan

From the article: "A new survey suggests the disruption, share price drops, and theft are common consequences of attacks."

Source: https://www.zdnet.com/article/nearly-all-us-execs-have-experienced-a-cybersecurity-event-but-some-say-theres-still-no-plan/

UK Spy Chiefs Seal Cloud Data Deal With Amazon: FT

From the article: "UK intelligence agencies have entrusted classified data to Amazon's cloud computing arm AWS in a deal designed to vastly speed up their espionage capabilities, the Financial Times reported on Tuesday."

Source: https://www.securityweek.com/uk-spy-chiefs-seal-cloud-data-deal-amazon-ft

Third-party Data Breach Hits Singapore Healthcare Provider

From the article: "No IT systems or databases of the healthcare services provider were affected by the breach, it said in a report with both the police and Personal Data Protection Commission in Singapore."

Source: https://cyberintelmag.com/attacks-data-breaches/third-party-data-breach-hits-singapore-healthcare-provider/

Matrix for the masses platform Element One goes live: $5 a month with WhatsApp, Signal, Telegram bridges

From the article: "Element, which makes Matrix-based communications and collaboration tools, has launched a consumer-oriented version of its messaging platform, complete with bridges for WhatsApp, Signal and Telegram.…'

Source: https://go.theregister.com/feed/www.theregister.com/2021/10/26/element_one/

Wardrivers Can Still Easily Crack 70% of Wi-Fi Passwords

From the article: "Weaknesses in the current Wi-Fi standard and poorly chosen passwords allowed one wardriver to recover 70% of wireless network passwords."

Source: https://www.darkreading.com/attacks-breaches/wardrivers-can-still-crack-70-of-wifi-passwords

Australia drafts Online Privacy Bill to bolster data security

From the article: "Australia's Attorney-General has submitted the first draft of a new Online Privacy Bill that contains striking reforms over existing privacy laws."

Source: https://www.bleepingcomputer.com/news/security/australia-drafts-online-privacy-bill-to-bolster-data-security/

Simplifying Asset Management with Geolocation

From the article: "Asset management solutions through geolocation will play a critical role in connecting these devices and providing precise location management."

Source: https://www.iotforall.com/?p=132749

Link back to Table of Contents

Ransomware Gangs Exploiting Zero-Day Flaw in EntroLink VPN Appliances

From the article: "The EntroLink VPN appliances are being abused by multiple ransomware gangs after an exploit was released on an underground cybercrime forum in September 2021."

Source: https://cyberintelmag.com/attacks-data-breaches/ransomware-gangs-exploiting-zero-day-flaw-in-entrolink-vpn-appliances/

Pulling Back the Curtain on Bug Bounties

From the article: "It's critical that infosec professionals and consumers understand threats and vulnerabilities, but they are being kept in the dark."

Source: https://www.darkreading.com/vulnerabilities-threats/pulling-back-the-curtain-on-bug-bounties

Money launderers for Russian hacking groups arrested in Ukraine

From the article: "The Ukrainian cybercrime police force has arrested members of a group of money launderers and hackers at the request of U.S. intelligence services. "

Source: https://www.bleepingcomputer.com/news/security/money-launderers-for-russian-hacking-groups-arrested-in-ukraine/

Technology Does Not Transform Itself: The Role of Stakeholder Communication

From the article: "Including all stakeholders in the planning process of a project is vital to its successful execution. Including the end-user in communications gives a voice to the group most affected by development decisions."

Source: https://www.iotforall.com/technology-does-not-transform-itself-the-role-of-people-communication

Microsoft Warns About New Version of UpdateAgent Targeting Macs

From the article: "Security researchers at Microsoft Security Intelligence have discovered a new version of UpdateAgent (aka WizardUpdate) that targets Mac devices."

Source: https://cyberintelmag.com/malware-viruses/microsoft-warns-about-new-version-of-updateagent-targeting-macs/

Targets and Prizes Announced for 2022 ICS-Themed Pwn2Own

From the article: "The Zero Day Initiative (ZDI) on Monday announced the targets and prizes for the next Pwn2Own Miami hacking contest, which focuses on industrial control system (ICS) products and associated protocols."

Source: https://www.securityweek.com/targets-and-prizes-announced-2022-ics-themed-pwn2own

Microsoft is force installing PC Health Check in Windows 10

From the article: "Microsoft has begun force installing the PC Health Check application on Windows 10 devices using a new KB5005463 update."

Source: https://www.bleepingcomputer.com/news/microsoft/microsoft-is-force-installing-pc-health-check-in-windows-10/

5 Ways CMMC Security Requirements May Impact Universities

From the article: "The Cybersecurity Maturity Model Certification puts research universities in a position where they must validate the effectiveness of their security controls before applying for a grant or bidding on a government contract."

Source: https://www.darkreading.com/edge-articles/5-ways-cmmc-security-requirements-may-impact-universities

Researcher Explains Wi-Fi Password Cracking at Scale

From the article: "A security researcher at CyberArk was able to easily break more than 70 percent of Wi-Fi passwords he sniffed using relatively simple, cheap equipment."

Source: https://www.securityweek.com/researcher-explains-wi-fi-password-cracking-scale

Attackers Hijack Craigslist Emails to Bypass Security, Deliver Malware

From the article: "Manipulated Craigslist emails that abuse Microsoft OneDrive warn users that their ads contain ‘inappropriate content.”"

Source: https://threatpost.com/attackers-hijack-craigslist-email-malware/175754/

Illumio Brings Visibility, Zero Trust Principles to Hybrid Cloud

From the article: "A new product seeks to solve the two primary security issues that come with moving to the cloud: the danger of accidental misconfigurations and the loss of visibility."

Source: https://www.securityweek.com/illumio-brings-visibility-zero-trust-principles-hybrid-cloud

Why the Next-Generation of Application Security Is Needed

From the article: "New software and code stand at the core of everything we do, but how well is all of this new code tested? Luckily, autonomous application security is here."

Source: https://threatpost.com/next-generation-application-security/175765/

Are Baby Boomers More Vulnerable Online Than Younger Generations? You Might Be Surprised

From the article: "Growing up with computers and the Internet doesn't necessarily convey all the advantages often attributed to younger users."

Source: https://www.darkreading.com/vulnerabilities-threats/are-baby-boomers-more-vulnerable-online-than-younger-generations-you-might-be-surprised

Windows 10 KB5006738 released with fixes for printing issues

From the article: "Microsoft says this update and a separate Windows Server preview update will fix all outstanding printing issues affecting users since they mitigated the PrintNightmare vulnerabilities."

Source: https://www.bleepingcomputer.com/news/microsoft/windows-10-kb5006738-released-with-fixes-for-printing-issues/

Data Security: How Data Activity Monitoring Protects Against Ransomware

From the article: "To combat ransomware, data protection solutions need to play a role in your overall data security and cybersecurity strategy."

Source: https://securityintelligence.com/posts/data-security-data-activity-monitoring-ransomware/

Cheap and free cybersecurity training: 8 ways to build skills without breaking the bank

From the article: "Every organization wants to keep its employees’ cybersecurity skills up to date, but for many, the cost of advanced formal trainings can break the budget."

Source: https://www.csoonline.com/article/3340819/cheap-or-free-cybersecurity-training-resources.html

Putting cybersecurity first: Why secure-by-design must be the norm

From the article: "Organizations that aim to pull ahead of the competition need to develop a strong security culture from top to bottom."

Source: https://www.welivesecurity.com/2021/10/26/putting-cybersecurity-first-why-secure-by-design-must-be-norm/

Cybersecurity Talent Gap Narrows as Workforce Grows

From the article: "Job satisfaction and salaries have both increased for cybersecurity professionals, as younger workers seek specific training to prepare for a cybersecurity career."

Source: https://www.darkreading.com/careers-and-people/cybersecurity-talent-gap-narrows-as-workforce-grows

Public Clouds & Shared Responsibility: Lessons from Vulnerability Disclosure

From the article: "Much is made of shared responsibility for cloud security. But Oliver Tavakoli, CTO at Vectra AI, notes there's no guarantee that Azure or AWS are delivering services in a hardened and secure manner."

Source: https://threatpost.com/public-clouds-shared-responsibility-vulnerability/175778/

Britain Wants to Use Its New Cyber Command to 'Hunt' Ransomware Gangs

From the article: "The United Kingdom wants to use a recently formed cyber command to “hunt” and hack ransomware gangs, a high-level government official recently revealed."

Source: https://gizmodo.com/britain-wants-to-use-its-new-cyber-command-to-hunt-rans-1847930905

Uniform Spin Qubit Devices with Tunable Coupling in an All-Silicon 300 mm Integrated Process

From the article: "Larger arrays of electron spin qubits require radical improvements in fabrication and device uniformity."

Source: https://semiengineering.com/uniform-spin-qubit-devices-with-tunable-coupling-in-an-all-silicon-300-mm-integrated-process/

Singaporean minister touts internet 'kill switch' that finds kids reading net nasties and cuts 'em off ASAP

From the article: "A Minister in the Singapore government has suggested the creation of an internet kill switch that would prevent minors from reading questionable material online – perhaps using ratings of content created in real time by crowdsourced contributors."

Source: https://www.theregister.com/2021/10/27/ng_eng_hen_speech/

Protonmail celebrates Swiss court victory exempting it from telco data retention laws

From the article: "Encrypted email provider Protonmail has hailed a recent Swiss legal ruling as a "victory for privacy," after winning a lawsuit that sees it exempted from data retention laws in the mountainous realm.…"

Source: https://www.theregister.com/2021/10/27/protonmail_data_victory/

3D-IC Design Challenges And Requirements

From the article: "As demands accelerate for increasing density, higher bandwidths, and lower power, many IC design and packaging teams are taking a close look at vertical stacking multiple chips and chiplets."

Source: https://semiengineering.com/3d-ic-design-challenges-and-requirements/

The Road To Osmosis

From the article: "It's happening. Some may have speculated that, with the acquisition of OneSpin by Siemens, the OneSpin user group meeting, more commonly known as Osmosis, would be formally (pun intended) absorbed into a larger Siemens event."

Source: https://semiengineering.com/the-road-to-osmosis/

Hierarchical Verification for EC-FPGA Flow

From the article: "This document describes the methodology to apply EC-FPGA verification using hierarchical netlists."

Source: https://semiengineering.com/hierarchical-verification-for-ec-fpga-flow/

Blog Review: Oct. 27

From the article: "Siemens EDA's Ray Salemi continues looking into using Python for verification by looking at how pyuvm simplifies and refactors the UVM TLM system to take advantage of the fact that Python has multiple inheritance and no typing."

Source: https://semiengineering.com/blog-review-oct-27/

Co-Packaged Optics And The Evolution Of Switch/Optical Interconnects In Data Centers

From the article: "Driven by a need to reduce power and increase bandwidth density in data center network switches and other devices, the data networking industry is moving toward adoption of co-packaged optics (CPO)."

Source: https://semiengineering.com/co-packaged-optics-and-the-evolution-of-switch-optical-interconnects-in-data-centers/

Microchip Sees Significant Productivity Gains In Mature-Node Custom IC Design With In-Design Signoff DRC

From the article: "Microsemi pioneered the design of innovative chips that are used for multiple purposes across a variety of industries, using both mature and advanced process nodes."

Source: https://semiengineering.com/microchip-sees-significant-productivity-gains-in-mature-node-custom-ic-design-with-in-design-signoff-drc/

3D Printing For More Circuits

From the article: "Christopher Tuck, professor of material science at the University of Nottingham, observed that what’s particularly attractive among the many different processes and materials used for additive manufacturing (AM) is the ability to build up one layer at a time, which increases design flexibility."

Source: https://semiengineering.com/3d-printing-for-more-circuits/

5 steps to security incident response planning

From the article: "Breach disclosure has recently been in the news, and not necessarily in a good way."

Source: https://www.csoonline.com/article/3636985/5-steps-to-security-incident-response-planning.html

NIST's new devsecops guidance to aid transition to cloud-native apps

From the article: "The United States federal government, much like in industry, is moving toward cloud adoption, Devsecops and microservices-based architectures for cloud-native applications."

Source: https://www.csoonline.com/article/3637120/nists-new-devsecops-guidance-to-aid-transition-to-cloud-native-apps.html

Meet Balikbayan Foxes: a threat group impersonating the Philippine gov't

From the article: "The gang is also taking advantage of COVID-19 to propagate Trojan malware."

Source: https://www.zdnet.com/article/proofpoint-unmasks-balikbayan-foxes-a-threat-group-impersonating-the-philippine-govt/

Cost of a Data Breach: Retail Costs, Risks and More To Know

From the article: " That can include credit card numbers, names, addresses and, in the case of e-commerce data breaches, even passwords."

Source: https://securityintelligence.com/articles/cost-of-a-retail-data-breach/

ThycoticCentrify Integrates Secret Server With Privileged Access Management Platform

From the article: "Combination avails Secret Server customers to a range of SaaS services."

Source: https://www.darkreading.com/endpoint/thycoticcentrify-integrates-secret-server-with-privileged-access-management-platform

Avast Business Introduces Network Discovery for SMBs

From the article: "Combination avails Secret Server customers to a range of SaaS services."

Source: https://www.darkreading.com/perimeter/avast-business-introduces-network-discovery-for-smbs

Onfido Acquires EYN to Provide Acoustic-Based Liveness Detection

From the article: "Technology will be incorporated into Onfido's Real Identity Platform."

Source: https://www.darkreading.com/authentication/onfido-acquires-eyn-to-provide-acoustic-based-liveness-detection

Secondary Infektion, a Russian disinformation outfit, impersonated Swedish lawmaker

From the article: "A suspected Russian disinformation campaign used manipulated images and fabricated internet personas to promote false narratives online in an effort to sow mistrust in Sweden and Europe, according to new findings."

Source: https://www.cyberscoop.com/?p=59782

Telegram launches advertising program for public channels

From the article: "Telegram has launched a new advertising program dubbed Ad Platform and offering the opportunity to display sponsored messages on the instant-messaging platform."

Source: https://www.bleepingcomputer.com/news/software/telegram-launches-advertising-program-for-public-channels/

Cynerio Launches IoT Attack Detection and Response Module for Healthcare IoT Devices

From the article: "Module helps hospitals identify, contain, and mitigate threats on devices exhibiting malicious or suspicious behavior."

Source: https://www.darkreading.com/iot/cynerio-launches-iot-attack-detection-and-response-module-for-healthcare-iot-devices

Yubico Launches New Security Key With USB-C and NFC

From the article: "Yubico on Tuesday announced the launch of Security Key C NFC, a new hardware security key that includes NFC capabilities in a USB-C form factor."

Source: https://www.securityweek.com/yubico-launches-new-security-key-usb-c-and-nfc

How the FBI Gets Location Information

From the article: "Vice has a detailed article about how the FBI gets data from cell phone providers like AT&T, T-Mobile, and Verizon, based on a leaked (I think) 2019 139-page presentation."

Source: https://www.schneier.com/blog/archives/2021/10/how-the-fbi-gets-location-information.html

Annual Cyber Risk Survey Finds Businesses Are Sharpening Their Focus on Cybersecurity but Also Reveals Much Room for Improvement in Building Cyber-Resilience

From the article: "This year's survey features the highest percentage of cyber insurance buyers since the beginning of the survey 11 years ago."

Source: https://www.darkreading.com/risk/annual-cyber-risk-survey-finds-businesses-are-sharpening-their-focus-on-cybersecurity-but-also-reveals-much-room-for-improvement-in-building-cyber-resilience

Identity-Focused Security Controls Prevail

From the article: "How identity and access management strategies held up during the pandemic and tips for putting together an identity security road map."

Source: https://www.darkreading.com/operations/identity-focused-security-controls-prevail

Buried nanomagnet realizing high-speed/low-variability silicon spin qubits: implementable in error-correctable large-scale quantum computers

From the article: “We propose a buried nanomagnet (BNM) realizing highspeed/low-variability silicon spin qubit operation, inspired by buried wiring technology, for the first time."

Source: https://semiengineering.com/buried-nanomagnet-realizing-high-speed-low-variability-silicon-spin-qubits-implementable-in-error-correctable-large-scale-quantum-computers/

Small Dataset-Based Object Detection

From the article: "Object detection using computer vision can be performed with a small learning dataset if it aligns closely with the target objects. This is applicable in multiple industries, and has become more sophisticated in recent years."

Source: https://www.iotforall.com/small-dataset-based-object-detection

Five Industries Exploding Using Single SIM Technology

From the article: "When a cell network fails, IoT systems may follow — unless you use multi-carrier IoT SIM cards. Learn how single SIM technology is helping various industries."

Source: https://www.iotforall.com/five-industries-exploding-using-single-sim-technology

Materials and Device Simulations for Silicon Qubit Design and Optimization

From the article: “Silicon-based microelectronics technology is extremely mature, yet this profoundly important material is now also poised to become a foundation for quantum information processing technologies."

Source: https://semiengineering.com/materials-and-device-simulations-for-silicon-qubit-design-and-optimization/

SolarWinds Outlines 'Triple Build' Software Development Model to Secure Supply Chain

From the article: "When FireEye (now Mandiant) disclosed the SolarWinds breach in December 2020, the security world was forced to accept the reality that given the motivation, time and resources, an advanced attacker can breach any organization."

Source: https://www.securityweek.com/solarwinds-outlines-triple-build-software-development-model-secure-supply-chain

Fuji Electric Patches Vulnerabilities in Factory Monitoring Software

From the article: "Japanese electrical equipment company Fuji Electric has patched half a dozen types of vulnerabilities in its Tellus factory monitoring and operating product."

Source: https://www.securityweek.com/fuji-electric-patches-vulnerabilities-factory-monitoring-software

The Weaponization of Operational Technology

From the article: "Given the accelerating rise in operational technology (OT) threats, this blog will address some of the most common threats IBM Security X-Force is observing against organizations with OT networks, including ransomware and vulnerability exploitation."

Source: https://securityintelligence.com/posts/weaponization-operational-technology/

Cybercriminals Ramp Up Attacks on Web APIs

From the article: "As more organizations use application programming interfaces for Web applications, attacks and security incidents targeting APIs continue to grow."

Source: https://www.darkreading.com/threat-intelligence/cybercriminals-ramp-up-attacks-on-web-apis

6 Eye-Opening Statistics About Software Supply Chain Security

From the article: "The latest facts and figures on the state of software supply chain security in the enterprise."

Source: https://www.darkreading.com/application-security/6-eye-opening-statistics-about-software-supply-chain-security

Why Containers in the Cloud Can Be An Attacker's Paradise

From the article: "Containers — which are lightweight software packages that include entire runtime environments — have solved the issues of portability, compatibility and rapid, controlled deployment."

Source: https://securityintelligence.com/posts/containers-cloud-vulnerability-management/

Hackers arrested for 'infiltrating' Ukraine's health database

From the article: "The Security Service of Ukraine (SSU) has arrested a team of actors who illegally infiltrated the information system of the National Health Service of Ukraine (NHSU) and entered false vaccination entries for other people."

Source: https://www.bleepingcomputer.com/news/security/hackers-arrested-for-infiltrating-ukraine-s-health-database/

Twitter employees required to use security keys after 2020 hack

From the article: "Twitter rolled out security keys to its entire workforce and made two-factor authentication (2FA) mandatory for accessing internal systems following last year's hack."

Source: https://www.bleepingcomputer.com/news/security/twitter-employees-required-to-use-security-keys-after-2020-hack/

Read Between the Lines: Finding Flaws in EPUB Reading Systems

From the article: "Security researchers who analyzed 97 free EPUB reading applications found half are not compliant with security recommendations."

Source: https://www.darkreading.com/vulnerabilities-threats/read-between-the-lines-finding-flaws-in-epub-reading-systems

Malicious Roblox NPMs drop ransomware and password stealers

From the article: "Malicious NPM packages pretending to be Roblox libraries are delivering ransomware and password-stealing trojans on unsuspecting users."

Source: https://www.bleepingcomputer.com/news/security/malicious-roblox-npms-drop-ransomware-and-password-stealers/

DDoS VoIP Providers Coordinate Digital Extortions

From the article: "A trade group has issued a warning about a massive DDoS attack to extort money from Voice over IP (VoIP) providers globally."

Source: https://cyberintelmag.com/attacks-data-breaches/ddos-voip-providers-coordinate-digital-extortions/

Teen Rakes in $2.74M Worth of Bitcoin in Phishing Scam

From the article: "The kid was busted after abusing Google Ads to lure users to his fake gift card site."

Source: https://threatpost.com/teen-rakes-in-2-74m-worth-of-bitcoin-in-phishing-scam/175834/

NPM packages disguised as Roblox API code caught carrying ransomware

From the article: "Security firm Sonatype on Wednesday said it had spotted two related malicious NPM libraries that were named so they might be mistaken for a popular legitimate module that serves as a Roblox API wrapper."

Source: https://www.theregister.com/2021/10/27/npm_roblox_ransomware/

Defenders Worry Orgs Are More Vulnerable Than Last Year

From the article: "Most IT and security leaders are confident their cybersecurity strategies are on the right track, but they still believe their organizations are as vulnerable as they were a year ago."

Source: https://www.darkreading.com/edge-threat-monitor/defenders-worry-orgs-are-more-vulnerable-than-last-year

HelpSystems Acquires Digital Guardian, Extends DLP Capabilities

From the article: "The acquisition strengthens HelpSystems' data security portfolio with data loss prevention capabilities across the endpoint, network, and cloud."

Source: https://www.darkreading.com/cloud/helpsystems-acquires-digital-guardian-extends-dlp-capabilities

Customize Off-The-Shelf Processor IP

From the article: "Processor customization is one approach to optimizing a processor IP core to handle a certain workload."

Source: https://codasip.com/2021/10/01/processor-customization/

Functional Safety Across Analog And Digital Domains

From the article: "The autonomy of vehicles has been all the rage recently. There are different levels of autonomous driving, with level 5 “Full Automation” being the target the industry is working towards, and Level 2 “Partial Automation” and Level 3 “Conditional Automation” being the level at which the automotive sector currently delivers the most technology."

Source: https://semiengineering.com/functional-safety-across-analog-and-digital-domains/

Debug Solutions For Designers Accelerate Time To Verification

From the article: "Complexity continues to explode as designs become larger and more complicated with more functionality and more aggressive expectations."

Source: https://semiengineering.com/debug-solutions-for-designers-accelerate-time-to-verification/

Intelligent Coverage Optimization: Verification Closure In Hyperdrive

From the article: "Coverage dominates every aspect of verification for today’s complex IP and chip designs."

Source: https://semiengineering.com/intelligent-coverage-optimization-verification-closure-in-hyperdrive/

High-Level Synthesis For RISC-V

From the article: "High-quality RISC-V implementations are becoming more numerous, but it is the extensibility of the architecture that is driving a lot of design activity."

Source: https://semiengineering.com/high-level-synthesis-for-risc-v/

Partitioning For Better Performance And Power

From the article: "Partitioning is becoming more critical and much more complex as design teams balance different ways to optimize performance and power, shifting their focus from a single chip to a package or system involving multiple chips with very specific tasks."

Source: https://semiengineering.com/partitioning-for-better-performance-and-power/

What's Next For Emulation

From the article: "Emulation is now the cornerstone of verification for advanced chip designs, but how emulation will evolve to meet future demands involving increasingly dense, complex, and heterogeneous architectures isn't entirely clear."

Source: https://semiengineering.com/whats-next-for-emulation/

Dealing With Market Shifts

From the article: "We had gone from obscure new technology to market leader in just a few years, and it was almost the poster-boy for the company."

Source: https://semiengineering.com/dealing-with-market-shifts/

If your hair isn't already gray, 2022's security threats will get it there, warn infosec duo

From the article: "Those hoping for some respite from the world's ongoing woes are out of luck, apparently.…"

Source: https://www.theregister.com/2021/10/28/fireeye_mcafee_2022/

Android Spyware Apps Targeting Israeli Users Since 2018

From the article: "Researchers at Qihoo 360 uncovered the spyware-laden apps, which included Threema, Al-Aqsa Mosque, Al-Aqsa Radio, Jerusalem Guide, PDF reader, Wire, and other apps camouflaged as social apps."

Source: https://cyberintelmag.com/malware-viruses/android-spyware-apps-targeting-israeli-users-since-2018/

How disinformation creates insider threats

From the article: "As we enter quarter four of 2021, the idea of disinformation as a cyber threat probably hasn’t percolated to the forefront of concerns of many CISOs. Indeed, a Venn diagram would show no overlap of “disinformation” with the words “CISO” or “cyber threat,” especially in the United States."

Source: https://www.csoonline.com/article/3636993/how-disinformation-creates-insider-threats.html

Conti ransomware explained: What you need to know about this aggressive criminal group

From the article: "Researchers warn that unlike other ransomware groups that generally care about their reputation, Conti doesn't always deliver on its promises to victims."

Source: https://www.csoonline.com/article/3638056/conti-ransomware-explained-and-why-its-one-of-the-most-aggressive-criminal-groups.html

Crooks steal $130 million worth of cryptocurrency assets from Cream Finance

From the article: "Threat actors have stolen $130 million worth of cryptocurrency assets from the Cream Finance decentralized finance (DeFi) platform."

Source: https://securityaffairs.co/wordpress/123861/cyber-crime/cream-finance-cyber-heist-130m.html

Microsoft now rolling out Windows 11 to more eligible devices

From the article: "Microsoft is now rolling out the Windows 11 upgrade to more eligible Windows devices as part of a phased rollout designed to deliver a smooth upgrade experience."

Source: https://www.bleepingcomputer.com/news/microsoft/microsoft-now-rolling-out-windows-11-to-more-eligible-devices/

Roundup: 2021 Energy & Utility Data Breaches and Defenses in the News

From the article: "In May 2021, Colonial Pipeline, one of the largest fuel pipelines in the United States, faced a ransomware attack."

Source: https://securityintelligence.com/articles/energy-utility-data-breaches-2021/

You've Just Been Ransomed ... Now What?

From the article: "Six crucial steps executives and IT teams should be prepared to take immediately after a ransomware attack."

Source: https://www.darkreading.com/attacks-breaches/you-ve-just-been-ransomed---now-what-

AIoT: the Perfect Union Between the Internet of Things and Artificial Intelligence

From the article: "The true potential of the IoT can only be achieved through the introduction of Artificial Intelligence."

Source: https://www.iotforall.com/aiot-the-perfect-union-between-the-internet-of-things-and-artificial-intelligence

Federal CISO Chris DeRusha appointed deputy national cyber director, will serve both roles

From the article: "Federal Chief Information Security Officer Chris DeRusha, who has played an integral part in responding to the SolarWinds hack, is getting a second gig as deputy national cyber director for federal cybersecurity."

Source: https://www.cyberscoop.com/federal-ciso-chris-derusha-deputy-national-cyber-director/

Election officials don't need to report cyber incidents to the feds. That could soon change.

From the article: "Security personnel charged with the challenging and high-stakes work of protecting election systems from digital threats might soon have another task on their to-do list: reporting any cyber incidents to the federal government."

Source: https://www.cyberscoop.com/election-machine-hack-reporting-requirement-cisa/

EU’s Green Pass Vaccination ID Private Key Leaked

From the article: "UPDATE: French & Polish authorities found no sign of cryptographic compromise in the leak of the private key used to sign the vaccine passports and to create fake passes for Mickey Mouse and Adolf Hitler, et al."

Source: https://threatpost.com/eus-green-pass-vaccination-id-private-key-leaked/175857/

Link back to Table of Contents

How Shopping Bots Can Compromise Retail Cybersecurity

From the article: "Some customers use shopping bots to execute automated tasks based on a set of instructions, such as log onto website -> look for specific product -> add product to cart -> check out."

Source: https://securityintelligence.com/posts/shopping-bots-compromise-retail-cybersecurity/

Android spyware spreading as antivirus software in Japan

From the article: "A new variant of the Android info-stealer called FakeCop has been spotted by Japanese security researchers, who warn that the distribution of the malicious APK is picking up pace."

Source: https://www.bleepingcomputer.com/news/security/android-spyware-spreading-as-antivirus-software-in-japan/

Wslink, a previously undescribed loader for Windows binaries

From the article: "ESET researchers discovered a previously undescribed loader for Windows binaries, tracked as Wslink, that runs as a server and executes modules in memory."

Source: https://securityaffairs.co/wordpress/123878/malware/wslink-loader.html

3 Security Lessons Learned From the Kaseya Ransomware Attack

From the article: "Organizations can better prepare themselves and their customers for these attacks with some strategies to identify threats before they become a widespread issue."

Source: https://www.darkreading.com/attacks-breaches/3-security-lessons-learned-from-the-kaseya-ransomware-attack

US Dismisses Assange Suicide Risk in Extradition Appeal

From the article: "The United States urged two senior British judges on Wednesday to clear the extradition of WikiLeaks founder Julian Assange and reject a lower court's ruling that he is a suicide risk."

Source: https://www.securityweek.com/us-dismisses-assange-suicide-risk-extradition-appeal

Cisco Patches High-Severity DoS Vulnerabilities in ASA, FTD Software

From the article: "Cisco this week announced the release of a new set of security patches to address multiple vulnerabilities affecting Adaptive Security Appliance (ASA), Firepower Threat Defense (FTD), and Firepower Management Center (FMC) software."

Source: https://www.securityweek.com/cisco-patches-high-severity-dos-vulnerabilities-asa-ftd-software

3 Questions for MDRs Helping to Get Your Enterprise to XDR

From the article: "An XDR implementation can quickly turn into a very large consulting project requiring significant time and budget"

Source: https://www.securityweek.com/3-questions-mdrs-helping-get-your-enterprise-xdr

Vendor-Neutral Initiative Sets Bare-Minimum Baseline for Security

From the article: "Google on Wednesday announced the Minimum Viable Secure Product (MVSP) initiative, partnering with some of tech's biggest names to create a vendor-neutral minimum baseline criteria for secure products."

Source: https://www.securityweek.com/vendor-neutral-initiative-sets-bare-minimum-baseline-security

Critical GoCD Authentication Flaw Exposes Software Supply Chain

From the article: "A highly-critical vulnerability in a popular open-source CI/CD solution can be exploited to hijack sensitive secrets for downstream supply chain attacks, according to a warning from SonarSource."

Source: https://www.securityweek.com/critical-gocd-authentication-flaw-exposes-software-supply-chain

2021 Cyber Resilient Organization Study: Rise of Ransomware Shows the Need for Zero Trust and XDR

From the article: ""“How many millions did you pay threat actors in a ransomware attack?” “Which investments most significantly improved cyber resiliency for your organization?”"

Source: https://securityintelligence.com/posts/2021-cyber-resilient-organization-study/

Zales.com Leaked Customer Data, Just Like Sister Firms Jared, Kay Jewelers Did in 2018

From the article: "In December 2018, bling vendor Signet Jewelers fixed a weakness in their Kay Jewelers and Jared websites that exposed the order information for all of their online customers."

Source: https://krebsonsecurity.com/2021/10/zales-com-leaked-customer-data-just-like-sister-firms-jared-kay-jewelers-did-in-2018/

Identity and Access Management: What’s Driving the Rush?

From the article: "A recent Fortune Business Insights report projects that the global Identity and Access Management (IAM) market (valued at $9.53 billion in 2018) will reach $24.76 billion by the end of 2026, showing a CAGR of 13.17%."

Source: https://securityintelligence.com/articles/driving-rush-identity-access-management/

Stop Zero-Day Ransomware Cold With AI

From the article: "AI can help recognize ransomware attacks and stop them at computer speed."

Source: https://www.darkreading.com/emerging-tech/stop-zero-day-ransomware-cold-with-ai

US to Create Diplomatic Bureau to Lead Cybersecurity Policy

From the article: "As part of its modernization initiative, the Department of State will increase its IT budget by 50% and add a new bureau to lead cybersecurity and digital policy."

Source: https://www.darkreading.com/risk/us-to-create-diplomatic-bureau-to-lead-cybersecurity-policy

EU investigating leak of private key used to forge Covid passes

From the article: "The key has also been misused to generate forged certificates, such as those for Adolf Hitler, Mickey Mouse, Sponge Bob—all of which are being recognized as valid by the official government apps."

Source: https://www.bleepingcomputer.com/news/security/eu-investigating-leak-of-private-key-used-to-forge-covid-passes/

Sensitive data of 400,000 German students exposed by API flaw

From the article: "Approximately 400,000 users of Scoolio, a student community app widely used in Germany, had sensitive information exposed due to an API flaw in the platform."

Source: https://www.bleepingcomputer.com/news/security/sensitive-data-of-400-000-german-students-exposed-by-api-flaw/

Ransomware Attacks Are Evolving. Your Security Strategy Should, Too

From the article: "Defending against ransomware will take a move to zero-trust, argues Daniel Spicer, CSO, Ivanti."

Source: https://threatpost.com/ransomware-attacks-evolving-security-strategy/175835/

Wslink: Unique and undocumented malicious loader that runs as a server

From the article: "There are no code, functionality or operational similarities to suggest that this is a tool from a known threat actor"

Source: https://www.welivesecurity.com/2021/10/27/wslink-unique-undocumented-malicious-loader-runs-server/

Tech Companies Create Security Baseline for Enterprise Software

From the article: "The Minimum Viable Secure Product is written as a checklist of minimum-security requirements for business-to-business software."

Source: https://www.darkreading.com/application-security/tech-companies-create-security-baseline-for-enterprise-software

Ordr Unveils Cybersecurity Innovations and Ransom-Aware Rapid Assessment Service to Expand Its Leadership In Connected Device Security

From the article: "Enhanced ransomware detection, visualization of ransomware communications, and risk customization helps organizations respond to cyberattacks in minutes."

Source: https://www.darkreading.com/attacks-breaches/ordr-unveils-cybersecurity-innovations-and-ransom-aware-rapid-assessment-service-to-expand-its-leadership-in-connected-device-security

All Windows versions impacted by new LPE zero-day vulnerability

From the article: "A security researcher has disclosed technical details for a Windows zero-day privilege elevation vulnerability and a public proof-of-concept (PoC) exploit that gives SYSTEM privileges under certain conditions."

Source: https://www.bleepingcomputer.com/news/security/all-windows-versions-impacted-by-new-lpe-zero-day-vulnerability/

National Cyber Director Chris Inglis, new cyber kid on the federal block, begins to stake a claim

From the article: "National Cyber Director Chris Inglis is fleshing out what, exactly, his new office plans to do with itself."

Source: https://www.cyberscoop.com/chris-inglis-national-cyber-director-strategic-intent-statement/

FTC wants to know when financial data is compromised, will require encryption

From the article: "The Federal Trade Commission is weighing updating its rules to require financial institutions to report within 30 days any security incidents in which misuse of customer data of at least 1,000 customers likely occurred."

Source: https://www.cyberscoop.com/ftc-financial-breach-security/

All Sectors Are Now Prey as Cyber Threats Expand Targeting

From the article: "Aamir Lakhani, security researcher at Fortinet, says no sector is off limits these days: It's time for everyone to strengthen the kill chain."

Source: https://threatpost.com/cyber-threats-targeting-all-sectors/175873/

Hitachi, Trend Micro, Microsoft Japan Agreed to Collaborate on Security For Connected Cars

From the article: "Hitachi, Microsoft Japan, and Trend Micro Incorporated have agreed to collaborate on connected car security solutions."

Source: https://cyberintelmag.com/iot/hitachi-trend-micro-microsoft-japan-agreed-to-collaborate-on-security-for-connected-cars/

InstaVolt Selects Eseye to Deliver Ultra-Reliable Connectivity for its Nationwide UK Electric Vehicle Charge Point Network

From the article: "Eseye's advanced AnyNet+ eSIM and intelligent IoT Connectivity Platform has been selected by the UK's leading EV charge point network provider, InstaVolt, to deliver ultra-reliable cellular connectivity for its rapidly growing Electric Vehicle (EV) charging network across the UK."

Source: https://www.iotforall.com/?post_type=press-releases&p=135081

Microsoft: Windows web content filtering now generally available

From the article: "Microsoft has announced that web content filtering has reached general availability and is now available for all Windows enterprise customers."

Source: https://www.bleepingcomputer.com/news/microsoft/microsoft-windows-web-content-filtering-now-generally-available/

Ransomware Attack Hits PNG Finance Ministry

From the article: "A cyberattack on Papua New Guinea's finance ministry briefly disrupted government payments and operations, officials said late Thursday."

Source: https://www.securityweek.com/ransomware-attack-hits-png-finance-ministry

Automating Agriculture with Sensors

From the article: "Learn more about the various ways in which agriculture is automated to make smart farming more efficient and smooth with less man power."

Source: https://www.iotforall.com/?p=131746

Remote Work Security: Handling Setbacks in the Time of COVID-19

From the article: "Most security experts, IT workers and leaders understand that the pandemic brought a decline in business and digital safety."

Source: https://securityintelligence.com/articles/remote-work-security-solving-changes-covid-19/

Finding the Right Approach to Cloud Security Posture Management (CSPM)

From the article: "respond to new problems. Dr. Mike Lloyd, RedSeal's CTO, reviews one of the latest: CSPM."

Source: https://www.darkreading.com/cloud/finding-the-right-approach-to-cloud-security-posture-management-cspm-

A Treehouse of Security Horrors

From the article: "True-life horrors from conversations with software engineers and developers. D'oh!"

Source: https://www.darkreading.com/vulnerabilities-threats/a-treehouse-of-security-horrors

Decentralization at Scale: It's Time to Bring IoT and Blockchain Together

From the article: "Is the future of low-power connectivity for Consumer IoT and Industrial IoT use cases associated with decentralization and blockchain?"

Source: https://www.iotforall.com/?p=132221

UK data watchdog calls for end-to-end encryption across video chat apps by default

From the article: "Britain's new Information Commissioner has called for video conferencing companies to enable end-to-end encryption on their products – even as police managers and politicians condemn the technology and demand its removal."

Source:
https://www.theregister.com/2021/10/29/ico_end_to_end_encryption_call_video_apps/

Microsoft PowerToys adds Windows 11 theme, new mouse utility

From the article: "Microsoft has added new utilities to the PowerToys toolset and updated the user interface with a new Windows 11 theme for PowerRename."

Source: https://www.bleepingcomputer.com/news/microsoft/microsoft-powertoys-adds-windows-11-theme-new-mouse-utility/

HelpSystems Expands Shopping Spree With Digital Guardian Acquisition

From the article: "Minnesota-based IT management and software powerhouse HelpSystems expanded its year-long cybersecurity shopping spree with a new deal to acquire data loss prevention specialists Digital Guardian."

Source: https://www.securityweek.com/helpsystems-expands-shopping-spree-digital-guardian-acquisition

What Exactly Is Secure Access Service Edge (SASE)?

From the article: "Any company that supports a hybrid workforce should at least be familiar with this relatively new security approach."

Source: https://www.darkreading.com/edge-ask-the-experts/what-exactly-is-secure-access-service-edge-sase-

Google Chrome is Abused to Deliver Malware as 'Legit' Win 10 App

From the article: "Malware delivered via a compromised website on Chrome browsers can bypass User Account Controls to infect systems and steal sensitive data, such as credentials and cryptocurrency."

Source: https://threatpost.com/chrome-deliver-malware-as-legit-win-10-app/175884/

Data-breached Guntrader website calls in liquidators, is reborn as Guntrader 2 Ltd

From the article: "A British firearms sales website's owner has called in the liquidators as his company faces data breach lawsuits – while continuing to trade from a newly incorporated business.…"

Source: https://www.theregister.com/2021/10/29/guntrader_liquidators_order/

7 Ways to Improve Your Cybersecurity Team's Employee Satisfaction

From the article: "Your organization depends on your cybersecurity team to keep its infrastructure and data secure."

Source: https://securityintelligence.com/articles/jennifer-gregory/

Hive ransomware now encrypts Linux and FreeBSD systems

From the article: "The Hive ransomware gang now also encrypts Linux and FreeBSD using new malware variants specifically developed to target these platforms."

Source: https://www.bleepingcomputer.com/news/security/hive-ransomware-now-encrypts-linux-and-freebsd-systems/

Cybercriminals Take Aim at Connected Car Infrastructure

From the article: "While car makers are paying more attention to cybersecurity, the evolution of automobiles into "software platforms on wheels" and the quick adoption of new features has put connected cars in the crosshairs."

Source: https://www.darkreading.com/iot/cybercriminals-take-aim-at-connected-car-infrastructure

CISA starts identifying targets most necessary to protect from hacking

From the article: "The Cybersecurity and Infrastructure Security Agency has begun working to map out the U.S. critical infrastructure that, if hacked, could result in serious consequences for national security and economic interests, CISA Director Jen Easterly said Friday."

Source: https://www.cyberscoop.com/sici-easterly-katko-psies-csis-cisa/

GlobalFoundries IPO fails to impress Wall Street in first trading day

From the article: "Contract chip manufacturer GlobalFoundries did not have a picture-perfect beginning to its life as a public company Thursday, as sellers outnumbered buyers during the company's first trading day."

Source: https://www.protocol.com/bulletins/globalfoundries-ipo-stock

Chaos ransomware targets gamers via fake Minecraft alt lists

From the article: "The Chaos Ransomware gang encrypts gamers' Windows devices through fake Minecraft alt lists promoted on gaming forums."

Source: https://www.bleepingcomputer.com/news/security/chaos-ransomware-targets-gamers-via-fake-minecraft-alt-lists/

Apparent Iran-Linked Hackers Breach Israeli Internet Firm

From the article: "Hackers believed to be linked to Iran have breached an Israeli internet hosting company, taking down several of its sites, local media reported."

Source: https://www.securityweek.com/apparent-iran-linked-hackers-breach-israeli-internet-firm

Enterprises Allocating More IT Dollars on Cybersecurity

From the article: "Enterprises are allocating more IT dollars towards implementing a multilayered approach to securing data and applications against new threats, data shows."

Source: https://www.darkreading.com/tech-trends/enterprises-allocating-more-it-dollars-on-cybersecurity

Microsoft: Windows KB5006674, KB5006670 updates break printing

From the article: "Microsoft says Windows customers are experiencing issues with network printing after installing the Windows 11 KB5006674 and Windows 10 KB5006670 updates issued with this month's Patch Tuesday, on October 12."

Source: https://www.bleepingcomputer.com/news/microsoft/microsoft-windows-kb5006674-kb5006670-updates-break-printing/

ESET found a variant of the Hive ransomware that encrypts Linux and FreeBSD

From the article: "The Hive ransomware operators have developed a new variant of their malware that can encrypt Linux and FreeBSD."

Source: https://securityaffairs.co/wordpress/123931/malware/hive-ransomware-linux-freebsd.html

Snyk Agrees to Acquire CloudSkiff, Creators of driftctl

From the article: "New capabilities allow Snyk Infrastructure as Code customers to more effectively detect infrastructure drift."

Source: https://www.darkreading.com/application-security/snyk-agrees-to-acquire-cloudskiff-creators-of-driftctl

APTs, Teleworking, and Advanced VPN Exploits: The Perfect Storm

From the article: "A Mandiant researcher shares the details of an investigation into the misuse of Pulse Secure VPN devices by suspected state-sponsored threat actors."

Source: https://www.darkreading.com/threat-intelligence/apts-teleworking-and-advanced-vpn-exploits-the-perfect-storm

Papua New Guinea 's finance ministry was hit by a ransomware

From the article: "A ransomware attack hit Papua New Guinea 's finance ministry and disrupted government payments and operations."

Source: https://securityaffairs.co/wordpress/123927/cyber-crime/papua-new-guinea-ransomware.html

Fibocom: 5G AIoT Commercialized Products Handbook

From the article: "Fibocom "5G AIoT Commercialized Products Handbook" breaks the industry boundary with collective power and exploring new business value with technology integration."

Source: https://www.iotforall.com/ebooks/fibocom-5g-aiot-commercialized-products-handbook

Michigan police execute warrant looking for missing election equipment

From the article: "The Michigan State Police launched a criminal investigation this week after a piece of election equipment went missing."

Source: https://www.cyberscoop.com/michigan-police-execute-warrant-looking-for-missing-election-equipment/

Snake malware biting hard on 50 apps for only $25

From the article: "Cybercriminals are flooding to use the Snake password-stealing trojan, making it one of the popular malware families used in attacks."

Source: https://www.bleepingcomputer.com/news/security/snake-malware-biting-hard-on-50-apps-for-only-25/

Subscription

From Japan to U.S., thieves grab car parts worth more than gold

From the article: "In a city near Toyota Motor's hometown, police were recently confronted by a rare kind of theft, even for low-crime Japan. A Toyota Prius hybrid reported stolen last month in Nagakute, Aichi Prefecture, was later recovered with its catalytic converter cut out."

Source: https://asia.nikkei.com/Business/Markets/Commodities/From-Japan-to-U.S.-thieves-grab-car-parts-worth-more-than-gold

Intel's PC revenues dip amid component shortages and Apple Mac loss

From the article: “The chipmaker Intel disappointed Wall Street with its latest results outlook, saying that its clients were struggling to assemble notebook computers amid a global component shortage and that a Chinese crackdown on video gaming was hurting sales for data centers.”

Source: https://asia.nikkei.com/Business/Technology/Intel-s-PC-revenues-dip-amid-component-shortages-and-Apple-Mac-loss

Chip shortage stymies Rakuten's Japan mobile coverage

From the article: "Japanese e-commerce company Rakuten Group has again pushed back a coverage target for its bid to disrupt the country's wireless communications market, with a global chip shortage slowing progress on building its network."

Source: https://asia.nikkei.com/Business/Telecommunication/Chip-shortage-stymies-Rakuten-s-Japan-mobile-coverage

Taiwan foreign minister embarks on EU trip to bolster ties

From the article: "Taiwanese Foreign Minister Joseph Wu visits Central Europe this week as Taipei and the European Union pursue closer political ties along with economic partnerships in areas such as semiconductors."

Source: https://asia.nikkei.com/Politics/International-relations/Taiwan-foreign-minister-embarks-on-EU-trip-to-bolster-ties

SK Hynix sees rising demand for chips as quarterly profit surges

From the article: "SK Hynix forecast steady growth in demand for memory chips on Tuesday as it posted its highest quarterly operating profit since 2018 on the back of rising prices which offset slowing personal computer sales as COVID-19 lockdowns eased."

Source: https://asia.nikkei.com/Business/Tech/Semiconductors/SK-Hynix-sees-rising-demand-for-chips-as-quarterly-profit-surges

Hyundai Motor expects more chip shortage production disruptions

From the article: "Hyundai Motor said on Tuesday that a lack of computer chips for its vehicles will further disrupt production in the fourth quarter and into next year, casting a shadow over the South Korean car giant's global sales."

Source: https://asia.nikkei.com/Business/Automobiles/Hyundai-Motor-expects-more-chip-shortage-production-disruptions

Japan's Nidec focuses on EV motors as price battle heats up

From the article: "Japanese motor maker Nidec will focus on sales of motors for smaller electric vehicles, as intensifying price competition forces more automakers to source the vital components from outside suppliers, Nidec founder and Chairman Shigenobu Nagamori said Tuesday."

Source: https://asia.nikkei.com/Business/Electronics/Japan-s-Nidec-focuses-on-EV-motors-as-price-battle-heats-up

TSMC founder chides U.S. plan for full chip supply chain onshore

From the article: "As U.S. lawmakers look to invest $52 billion in the American chip industry, the founder of Taiwan Semiconductor Manufacturing Co. calls the plan far too small for rebuilding a complete supply chain in the country."

Source: https://asia.nikkei.com/Business/Tech/Semiconductors/TSMC-founder-chides-U.S.-plan-for-full-chip-supply-chain-onshore

Apple's clean energy drive draws more Asian suppliers

From the article: "Apple now counts 175 suppliers that have committed to using 100% renewable energy to produce components and assemble for its products, the company announced Wednesday, as the global push for decarbonization sweeps the technology sector."

Source: https://asia.nikkei.com/Business/Technology/Apple-s-clean-energy-drive-draws-more-Asian-suppliers

Chipmaker GlobalFoundries prices IPO at upper end to raise $2.6bn

From the article: "Chipmaker GlobalFoundries said on Wednesday it sold shares in its initial public offering at $47 a piece, at the higher end of its targeted price range, to raise about $2.6 billion."

Source: https://asia.nikkei.com/Business/Markets/IPO/Chipmaker-GlobalFoundries-prices-IPO-at-upper-end-to-raise-2.6bn

German chipmaker Infineon calls for rethink of auto supply chain

From the article: "German chip giant Infineon Technologies is urging automakers to rethink their "just-in-time" supply chain strategy and instead start building up stockpiles of semiconductors as the global shortage of the key components drags on."

Source: https://asia.nikkei.com/Editor-s-Picks/Interview/German-chipmaker-Infineon-calls-for-rethink-of-auto-supply-chain

Samsung plans to triple foundry chip production capacity by 2026

From the article: "Samsung Electronics said Thursday that it plans to triple its foundry production capacity by 2026 amid a global chip shortage disrupting production in key industries from autos to smartphones as it reported strong third quarter earnings."

Source: https://asia.nikkei.com/Business/Technology/Samsung-plans-to-triple-foundry-chip-production-capacity-by-2026

Weak yen is 'positive' for Japan's economy: BOJ Kuroda

From the article: "The yen's recent slide to a three-year low against the dollar has Japan worried that this could hurt business and consumer sentiment by making things more expensive amid skyrocketing commodity prices. But on Thursday, Bank of Japan Gov. Haruhiko Kuroda dismissed this, saying a weak yen does more good than harm."

Source: https://asia.nikkei.com/Economy/Weak-yen-is-positive-for-Japan-s-economy-BOJ-Kuroda

Sony confirms possible TSMC partnership on Japan chip factory

From the article: "Sony Group on Thursday confirmed it is considering a plan to join with Taiwan Semiconductor Manufacturing Co. in building a chip factory in the western Japanese prefecture of Kumamoto."

Source: https://asia.nikkei.com/Business/Media-Entertainment/Sony-confirms-possible-TSMC-partnership-on-Japan-chip-factory

Apple warns of more supply chain woes after $6bn revenue hit

From the article: "Apple posted record September-quarter revenue of $83.4 billion on Thursday, driven by sales of 5G iPhones, especially in the Chinese-speaking world, but would have made billions more if not for the supply chain bottlenecks plaguing the global tech sector."

Source: https://asia.nikkei.com/Business/Technology/Apple-warns-of-more-supply-chain-woes-after-6bn-revenue-hit

Top U.S. diplomat in Taiwan stresses supply chain cooperation

From the article: "The U.S. will work closely with Taiwan to build "resilient" and "safe" supply chains, Washington's top diplomat in Taipei said on Friday, as she also sought to ease concerns over a recent U.S. request for the island's chipmakers to hand over sensitive data."

Source: https://asia.nikkei.com/Economy/Trade-war/Top-U.S.-diplomat-in-Taiwan-stresses-supply-chain-cooperation

Mitsubishi Heavy aims for low-carbon shift after profit rebound

From the article: "Mitsubishi Heavy Industries returned to profit in the six months through September despite sluggish sales, as the company works to transform itself into a leader in decarbonation technology."

Source: https://asia.nikkei.com/Business/Companies/Mitsubishi-Heavy-aims-for-low-carbon-shift-after-profit-rebound

Taiwan's Wu urges partners to step up South China Sea exercises

From the article: "Ahead of a visit by his Chinese counterpart to the Italian capital for G-20 meetings, Taiwanese Foreign Minister Joseph Wu used a virtual address to Rome on Friday to berate Beijing over recent belligerent actions toward the democratic island."

Source: https://asia.nikkei.com/Spotlight/G-20-summit-2/Taiwan-s-Wu-urges-partners-to-step-up-South-China-Sea-exercises

Taiwan struggles to balance high-tech and low-carbon ambitions

From the article: "Asia's efforts to hit international greenhouse gas emission cuts targets have come under pressure from powerful industry lobbies, fossil fuel dependence and lack of investment in renewable energy sources in poor countries."

Source: https://asia.nikkei.com/Spotlight/Environment/Climate-Change/Asia-s-climate-crisis/Taiwan-struggles-to-balance-high-tech-and-low-carbon-ambitions

An Apparent Ransomware Hack Puts the NRA in a Bind

Summary: Wired dives into the ransomware gang responsible for the NRA ransomware attack last month.

Source: https://www.wired.com/story/nra-ransomware-hack-sanctions-payment/

Russian Hackers Used Home Networks to Evade Detection

Summary: Bloomberg article on technique used by Russian hackers to use 'home networks' to evade detection

Source: https://www.bloomberg.com/news/articles/2021-10-26/suspected-russian-hackers-use-home-networks-to-evade-detection

Top Chipmaker TSMC Rebuffs U.S. Request for Supply Chain Information

From the article: "Taiwan Semiconductor Manufacturing Co. Ltd. (TSMC), the world's largest contract chipmaker, said that it will not hand over "confidential client information" to the U.S. government, in a latest response to Washington's request for chip firms to share their supply chain data amid a global semiconductor shortage."

Source: https://www.caixinglobal.com/2021-10-27/top-chipmaker-tsmc-rebuffs-us-request-for-supply-chain-information-101792441.html