Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

Daily Open-Source Cyber Report

November 18, 2024

Extracted from multiple sources by PT and OTRB, and ST ISAC analysts for the purpose of supporting ISAC member cybersecurity awareness, protection, and mitigation.

Recipients may share this report only within their own immediate organization. No further dissemination is authorized.

Critical Infrastructure Security and Resilience Month

Shields Ready

The "Shields Ready" campaign is about making resilience during incidents a reality by taking action before incidents occur. As a companion to CISA's "Shields Up" initiative, Shields Ready drives action at the intersection of critical infrastructure resilience and national preparedness. This campaign is designed to help all critical infrastructure stakeholders take action to enhance security and resilience—from industry and businesses to government entities at all levels, and even individuals by providing recommendations, products, and resources to increase individual and collective resilience for different risk contexts and conditions. By taking steps before an incident, organizations, individuals, and communities are better positioned to quickly adjust their posture for heightened risk conditions, helping to prevent incidents, reduce impact, and get things back to normal—or better—as quickly as possible. To learn more, visit: https://www.cisa.gov/shields-ready

AT-A-GLANCE

EXECUTIVE NEWS

Trend Micro and Japanese Partners Reveal Hidden Connections Among SEO Malware Operations
Trend Micro, 11/11/2024

Trend Micro researchers recently conducted a research project that analyzed the relationship among multiple blackhat search engine optimization (SEO) malware families. By analyzing data from command-and-control (C&C) servers of different types of SEO malware and fake shopping sites, they were able to identify distinct groups of SEO malware families, how these share infrastructure to maximize the effectiveness of SEO poisoning attacks, and their role in orchestrating e-commerce scams. This project was carried out in partnership with Japanese several organizations, namely Kagawa University, Kanagawa Prefectural Police Headquarters, Chiba Prefectural Police Headquarters, and Japan Cybercrime Control Center (JC3). Their research paper titled.
https://www.trendmicro.com/en_us/research/24/k/seo-malware.html

Warning: Online Shopping Threats To Avoid This Black Friday and Cyber Monday
MalwareBytes, 11/13/2024

It's that time of year again. Thanksgiving will pass just as quickly as it arrived, and the festive season will soon hit full swing as countless people go online for some gift shopping. But where there's a gift to be bought, there's also a scammer out to make money. And make money they do. In the last five years, the Internet Crime Complaint Center (IC3) said it has received 3.79 million complaints for a wide range of internet scams, resulting in $37.4 billion in losses. Today, we're warning of several online threats that could target you over the next few weeks and months: brand impersonation and fakes, credit card skimming, and malvertising. https://www.malwarebytes.com/blog/news/2024/11/warning-online-shopping-threats-to-avoid-this-black-friday-and-cyber-monday

Innovative New Cyber Clinic Equips Canada's Non-Profits To Combat Growing Cyber Threats
CISA, 11/14/2024

Rogers Cybersecure Catalyst at Toronto Metropolitan University is proud to announce the launch of the Catalyst Cyber Clinic ("the Cyber Clinic"). The Cyber Clinic will offer free cybersecurity services to under-resourced not-for-profit organizations in Canada, and will be staffed by cybersecurity learners and graduates who, by working at the Cyber Clinic, will gain the hands-on cybersecurity experience they need to find employment in cybersecurity. Rogers Cybersecure Catalyst is grateful to computing leader Okta, which is powering this vital initiative through a major donation from its philanthropic arm, Okta for Good. Okta for Good's significant contribution will support the launch of the Catalyst Cyber Clinic and its initial program deliveries. https://www.newswire.ca/news-releases/innovative-new-cyber-clinic-equips-canada-s-non-profits-to-combat-growing-cyber-threats-886381511.html

Here's How Misconfigurations In Microsoft Power Pages Could Lead To Data Breaches
Cyber Scoop, 11/14/2024

Microsoft's Power Pages is a low-code platform that enables users to create data-driven websites with minimal coding requirements or knowledge. It's used by both the public and private sector, at organizations large and small, to assist in all sorts of scenarios where a customer or a citizen needs data to solve a problem. These pages also may be creating a problem for their respective organizations, in the form of leaking sensitive information, if they are not configured correctly. Researchers at Software-as-a-Service (SaaS) security company AppOmni discovered exactly how this happens within Power Pages, which has been detailed in research published Thursday. https://cyberscoop.com/microsoft-power-pages-misconfiguration-appomni/

6 Principles of Operational Technology Cybersecurity released by joint NSA initiative
Security Intelligence, 11/9/2024

Today's critical infrastructure organizations rely on operational technology (OT) to help control and manage the systems and processes required to keep critical services to the public running. However, due to the highly integrated nature of OT deployments, cybersecurity has become a primary concern. On October 2, 2024, the NSA (National Security Agency) released a new CSI titled "Principles of Operational Technology Cybersecurity." This new guide was created in collaboration with the Australian Signals Directorate's Australian Cyber Security Centre (ASD SCSC) to help promote best practices in security OT environments. https://securityintelligence.com/posts/6-principles-operational-technology-cybersecurity-nsa-initiative/

The Importance of Effective Incident Response
Hack Read, 11/11/2024

With cybersecurity threats continuously evolving, having a strong incident response (IR) plan is crucial for businesses of all sizes. Effective IR not only minimizes the financial and reputational damage caused by security incidents but also ensures that organizations can return to normal operations without delay. Here's why Incident Response is essential and what it entails. When a cyber incident strikes, the faster an organization can identify, contain, and mitigate it, the lower the financial losses. An effective IR plan enables businesses to respond efficiently, which helps reduce costly downtime, potential ransom demands, and expenses related to data recovery. https://hackread.com/the-importance-of-effective-incident-response/

Quantum Technologies Could Have £8 Billion of Impact on UK Transport by 2035
Quantum Insider, 11/15/2024

Quantum technologies could generate up to £8 billion in economic value for the UK transport sector by 2035, according to a report from the Department for Transport (DfT). While there is a proverbial long road ahead, the study explores how advances in quantum computing, communication and sensing could tackle long-standing challenges in the industry, from optimizing traffic flow to protecting critical infrastructure from cyberattacks. The team, which includes analysts from Resonance, reports that, although these technologies remain at varying levels of development, they offer transformative potential in a range of transportation-related uses. https://thequantuminsider.com/2024/11/15/quantum-technologies-could-have-8-billion-of-impact-on-uk-transport-by-2035/

TECHNICAL SUMMARY

EMERGING THREATS & EXPLOITS

- ***New Ymir Ransomware Partners With Rustystealer In Attacks*** - A new ransomware family called 'Ymir' has been spotted in the wild, encrypting systems that were previously compromised by the RustyStealer infostealer malware. RustyStealer is a known malware family first documented in 2021, but its appearance with ransomware demonstrates another example of the recent trend of cybercrime operations working together. https://www.bleepingcomputer.com/news/security/new-ymir-ransomware-partners-with-rustystealer-in-attacks/
- ***Flexible Structure of Zip Archives Exploited to Hide Malware Undetected*** - Threat actors are exploiting the various ways that zip files combine multiple archives into one file as an anti-detection tactic in phishing attacks that deliver various Trojan malware strains, including SmokeLoader. https://www.darkreading.com/threat-intelligence/flexible-structure-zip-archives-exploited-hide-malware-undetected
- ***Microsoft Visio Files Used in Sophisticated Phishing Attacks*** **-** A surge in two-step phishing attacks leveraging Microsoft Visio files has been identified by security researchers, marking a sophisticated evolution in phishing tactics. Discovered by Perception Point, the new attacks use Visio's .vsdx format, a file type commonly employed for business diagrams, to disguise malicious URLs and bypass traditional security scans. https://www.infosecurity-magazine.com/news/microsoft-visio-files-phishing/
- ***A New Fileless Variant Of Remcos RAT Observed In The Wild –*** Fortinet researchers discovered a new phishing campaign spreading a variant of the commercial malware Remcos RAT. Remcos is a commercial remote administration tool (RAT) that is sold online to allow buyers remote control over computers. Threat actors use Remcos to steal sensitive information and control victims' computers for malicious activities. https://securityaffairs.com/170791/cyber-crime/a-new-fileless-variant-of-remcos-rat-phishing.html
- ***Security Flaws in Popular ML Toolkits Enable Server Hijacks, Privilege Escalation -*** Cybersecurity researchers have uncovered nearly two dozen security flaws spanning 15 different machine learning (ML) related open-source projects. These comprise vulnerabilities discovered both on the server- and client-side, software supply chain security firm JFrog said in an analysis published last week. https://thehackernews.com/2024/11/security-flaws-in-popular-ml-toolkits.html

ATTACKS, BREACHES & LEAKS

- ***Chinese Salt Typhoon Hacked T-Mobile in U.S. Telecom Breach Spree -*** Another day, another hack at T-Mobile! This time, Chinese state-sponsored group Salt Typhoon hacked T-Mobile, targeting US telecoms in a breach spree. The attack exposes vulnerabilities in telecom infrastructure and security. https://hackread.com/chinese-salt-typhoon-hacked-t-mobile-telecom-breach/
- ***Klarenbeek Transport Data Breach*** - Klarenbeek Transport specializes in refrigerated transport and offers various other solutions to meet your transportation needs. https://www.breachsense.com/breaches/klarenbeek-transport-data-breach/
- ***Foreign Adversary Hacked Email Communications Of The Library Of Congress Says*** - The Library of Congress informed lawmakers about a security breach, an alleged foreign adversary compromised some of their IT systems and gained access to email communications between congressional offices and some library staff, including the Congressional Research Service. https://securityaffairs.com/171138/data-breach/library-of-congress-email-communications-hacked.html
- ***Ransomware Group BlackSuit Hits: brandywinecoachworks.com*** - https://www.hookphish.com/blog/ransomware-group-blacksuit-hits-brandywinecoachworks-com/
- ***Chinese Hackers Target Tibetan Websites in Malware Attack, Cybersecurity Group Says -*** A hacking group that is believed to be Chinese state-sponsored has compromised two websites with ties to the Tibetan community in an attack meant to install malware on users' computers, according to findings released Wednesday by a private cybersecurity firm. https://www.securityweek.com/chinese-hackers-target-tibetan-websites-in-malware-attack-cybersecurity-group-says/

SECURITY VULNERABILITIES, ALERTS, ADVISORIES, & UPDATES

SUSE SECURITY UPDATES

1. Salt –
   a. https://www.suse.com/support/update/announcement/2024/suse-ru-20244033-1
   b. https://www.suse.com/support/update/announcement/2024/suse-ru-20244032-1
   c. https://www.suse.com/support/update/announcement/2024/suse-ru-20244031-1
2. Expat - https://www.suse.com/support/update/announcement/2024/suse-su-20244035-1
3. SUSE Manager Salt Bundle –
   a. https://www.suse.com/support/update/announcement/2024/suse-su-20244025-1
   b. https://www.suse.com/support/update/announcement/2024/suse-su-20244029-1
   c. https://www.suse.com/support/update/announcement/2024/suse-su-20244025-1
   d. https://www.suse.com/support/update/announcement/2024/suse-su-20244021-1

GENTOO SECURITY ADVISORIES

1. Perl - https://security.gentoo.org/glsa/202411-09
2. X.Org X server, XWayland - https://security.gentoo.org/glsa/202411-08
3. Pillow - https://security.gentoo.org/glsa/202411-07

FEDORA SECURITY ADVISORIES

1. dotnet9.0 - https://lwn.net/Articles/998532
2. ghostscript –
   a. https://lwn.net/Articles/998534
   b. https://lwn.net/Articles/998533
3. php-bartlett-PHP-CompatInfo - https://lwn.net/Articles/998536
4. microcode_ctl - https://lwn.net/Articles/998535

MAGEIA SECURITY ADVISORIES

1. nvidia -current - http://advisories.mageia.org/MGAA-2024-0231.html

CHECK POINT SECURITY ADVISORIES

1. Palo Alto - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-0954.html

SENSITIVE & PROPRIETARY INFROMATION - NOT FOR PUBLIC DISSEMINATION

If you have any questions about this document please contact the ISAC at 866-ST-ISAC1 (866.784.7221) or email st-isac@surfacetransportationisac.org

2. https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-0949.html
3. PDF.js Cross-Site Scripting - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-0348.html

Red Hat Security Advisories

1. squid:4 - https://access.redhat.com/errata/RHSA-2024:9813
2. tigervnc - https://access.redhat.com/errata/RHSA-2024:9816
3. libvpx - https://access.redhat.com/errata/RHSA-2024:9827

Ubuntu Security Notices

1. Glib - https://ubuntu.com/security/notices/USN-7114-1
2. Curl - https://ubuntu.com/security/notices/USN-7104-1
3. WebKitGTK - https://ubuntu.com/security/notices/USN-7113-1
4. AsyncSSH - https://ubuntu.com/security/notices/USN-7108-1

Zero Day Initiative Advisories & Updates

1. Progress Software WhatsUp - https://www.zerodayinitiative.com/advisories/ZDI-24-1512/

Oracle Linux Security Update

1. Giflib - https://lwn.net/Articles/998548
2. Binutils - https://lwn.net/Articles/998544
3. Giflib - https://lwn.net/Articles/998547

Other

1. PHP-CGI Argument Injection Susceptibility Scanner - https://packetstormsecurity.com/files/download/182662/CVE-2024-4577-checker-main.zip

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

SENSITIVE & PROPRIETARY INFROMATION - NOT FOR PUBLIC DISSEMINATION

If you have any questions about this document please contact the ISAC at 866-ST-ISAC1 (866.784.7221) or email st-isac@surfacetransportationisac.org