Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

Daily Open-Source Cyber Report

December 26, 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.

AT-A-GLANCE

Executive News

- CISA Orders Federal Agencies To Secure Their Microsoft Cloud Environments
- China Target Of New U.S. Freight Car Security Rule
- EU Sanctions Russian Cyber Actors for "Destabilizing Actions"
- New Android Novispy Spyware Linked To Qualcomm Zero-Day Bugs
- Court Indicts 14 North Korean It Workers Tied To $88 Million In Illicit Gains
- Manufacturing Sector Most Targeted By Cyber Threat Actors During Q3
- APIs Risk Attack Mere Seconds After Deployment, Researchers Say

Emerging Threats & Vulnerabilities

- Citrix Shares Mitigations For Ongoing Netscaler Password Spray Attacks
- Undocumented DrayTek Vulnerabilities Exploited to Hack Hundreds of Orgs
- The Mask APT Resurfaces with Sophisticated Multi-Platform Malware Arsenal
- Hackers Use Fake PoCs on GitHub to Steal WordPress Credentials, AWS Keys
- Link Trap: GenAI Prompt Injection Attack

Attacks, Breaches, & Leaks

- Lazarus Apt Targeted Employees At An Unnamed Nuclear-Related Organization
- Investigation underway after Pittsburgh Regional Transit alerts riders of cybersecurity incident
- Circle Electric Data Breach
- Cicada3301 Ransomware Claims Attack on French Peugeot Dealership
- Tracker firm Hapn spilled names of thousands of GPS tracking customers

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

EXECUTIVE NEWS

CISA Orders Federal Agencies To Secure Their Microsoft Cloud Environments
Next Gov, 12/16/2024

"In the future, CISA may release additional SCuBA Secure Configuration Baselines for other cloud products," the agency explained. "As of December 2024, CISA has released finalized SCBs for Microsoft 365 (which is in scope for the BOD at issuance) and draft SCBs for Google Workspace (which are anticipated to enter scope in Q2, FY 2025)." Secure configuration baselines for Microsoft 365 cloud services include those related to Azure AD/Entra ID, Microsoft Defender, Exchange Online, Power Platform, SharePoint Online & OneDrive, and Microsoft Teams. As new updates to mandatory SCuBA policies are released, agencies must implement them by the due dates set by CISA.
https://www.helpnetsecurity.com/2024/12/19/cisa-bod-25-01-directive-secure-microsoft-cloud-environments/

China Target Of New U.S. Freight Car Security Rule
Freight Waves, 12/20/2024

The Federal Railroad Administration has issued a new final rule on freight car safety standards including limitations on cars or parts from China or another "country of concern." The rule, released Thursday and effective Jan. 21, 2025, fulfills a requirement of the Infrastructure Investment and Jobs Act. The rule requires railcars to be manufactured or assembled in "a qualified facility by a qualified manufacturer." In addition to limiting components from countries of concern or state-owned enterprises in such countries, it bars essential components or sensitive technology from such countries and enterprises. Penalties include prohibiting manufacturers from supplying freight cars for U.S. use.
https://www.freightwaves.com/news/china-target-of-new-us-freight-car-security-rule

EU Sanctions Russian Cyber Actors for "Destabilizing Actions"
Infosecurity Magazine, 12/17/2024

The European Union (EU) has announced sanctions against Russian cyber actors for carrying out attacks and disinformation campaigns abroad. The European Council imposed measures against 16 individuals and three entities described as undertaking "destabilizing actions abroad" on behalf of the Russian state. It is the first time the intragovernmental agency has issued sanctions under a framework set up in October 2024, with the EU condemning the Kremlin's "intensifying campaign of hybrid activities" when the powers were agreed. All organizations and individuals designated under the new sanctions will be subject to an asset freeze and EU citizens and companies will be forbidden from making funds available to them. https://www.infosecurity-magazine.com/news/eu-sanctions-russian-cyber-actors/

New Android Novispy Spyware Linked To Qualcomm Zero-Day Bugs
Bleeping Computer, 12/16/2024

The Serbian government exploited Qualcomm zero-days to unlock and infect Android devices with a new spyware named 'NoviSpy,' used to spy on activists, journalists, and protestors. One of the Qualcomm flaws linked to the attacks is CVE-2024-43047, which was marked as an actively exploited zero-day vulnerability by Google Project Zero in October 2024 and received a fix on Android in November. The spyware, which appears to have been deployed by Serbian authorities, based on its communications, was discovered by Amnesty International's Security Lab on a journalist's phone after police returned it. "In February 2024, Slaviša Milanov, an independent journalist from Dimitrovgrad in Serbia who covers local interest news stories, was brought into a police station after a seemingly routine traffic stop," reads a report by Amnesty International.
https://www.bleepingcomputer.com/news/security/new-android-novispy-spyware-linked-to-qualcomm-zero-day-bugs/

Court Indicts 14 North Korean It Workers Tied To $88 Million In Illicit Gains
Cyber Scoop, 12/12/2024

A federal court has indicted 14 more North Korean IT workers as part of an ongoing U.S. government campaign to crack down on Pyongyang's use of tech professionals to swindle American companies and nonprofits. The Justice Department said the 14 indicted workers generated at least $88 million throughout a conspiracy that stretched over approximately six years, ending in March 2023. North Korea-controlled companies in China and Russia — Yanbian Silverstar and Volasys Silverstar, respectively — used the so-called "IT Warriors" to obtain false U.S. identities, pose as employees doing remote IT work in the United States and transfer funds from their employers to eventually end up in the hands of the North Korean government, according to the indictment. https://cyberscoop.com/court-indicts-14-north-korean-it-workers-tied-to-88-million-in-illicit-gains/

Manufacturing Sector Most Targeted By Cyber Threat Actors During Q3
EMS Now, 12/15/2024

London, UK– Leading industrial cybersecurity solutions provider, Dragos has revealed manufacturing as the most likely industrial sector to fall victim to cyber-attacks, with the sector facing 394 unique attacks across Q3 2024 – 71% of all ransomware incidents across key industries. Dragos assesses with moderate confidence that ransomware activity targeting industrial organisations will continue to escalate into the future, driven by financially and ideologically motivated actors. The shift from traditional financial extortion to operational sabotage, particularly by hacktivist personas, compounds these risks. This convergence of motivations further blurs the line between cybercrime and cyberwarfare, requiring enhanced defenses for ICS and OT environments. https://www.emsnow.com/manufacturing-sector-most-targeted-by-cyber-threat-actors-during-q3/

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

APIs Risk Attack Mere Seconds After Deployment, Researchers Say
SC Media, 12/17/2024

Developers deploying APIs face the danger of automated attacks and exploits just seconds after deployment. Researchers from security vendor Wallarm performed a first-of-its-kind "honeypot" study in which a group of servers were equipped with a Golang API and left open to all ports in 14 locations. What they found was a waiting and ready environment of attackers ready to pounce on the servers and their underlying APIs with probes and exploit attempts. API exploit code was almost as common as web-based attacks, comprising 48% of exploit attempts. "Newly deployed APIs are often less protected, unmanaged, and less secure," wrote the the Wallarm team. https://www.scworld.com/news/apis-risk-attack-less-than-one-minute-from-deployment

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

TECHNICAL SUMMARY

EMERGING THREATS & EXPLOITS

- ***Citrix Shares Mitigations For Ongoing Netscaler Password Spray Attacks -*** Citrix Netscaler is the latest target in widespread password spray attacks targeting edge networking devices and cloud platforms this year to breach corporate networks. https://www.bleepingcomputer.com/news/security/citrix-shares-mitigations-for-ongoing-netscaler-password-spray-attacks/
- ***Undocumented DrayTek Vulnerabilities Exploited to Hack Hundreds of Orgs*** - More than 300 organizations were hacked by ransomware groups using undocumented vulnerabilities in DrayTek devices, including a potential zero-day flaw, according to a warning from cybersecurity vendor Forescout. https://www.securityweek.com/undocumented-draytek-vulnerabilities-exploited-to-hack-hundreds-of-orgs/
- ***The Mask APT Resurfaces with Sophisticated Multi-Platform Malware Arsenal -*** A little-known cyber espionage actor known as The Mask has been linked to a new set of attacks targeting an unnamed organization in Latin America twice in 2019 and 2022. https://thehackernews.com/2024/12/the-mask-apt-resurfaces-with.html
- ***Hackers Use Fake PoCs on GitHub to Steal WordPress Credentials, AWS Keys –*** Datadog Security Labs' cybersecurity researchers have discovered a new, malicious year-long campaign from a threat actor identified as MUT-1244, which resulted in the theft of over 390,000 WordPress credentials. https://hackread.com/hackers-fake-pocs-github-wordpress-credentials-aws-keys/
- ***Link Trap: GenAI Prompt Injection Attack –*** With the rise of generative AI, new security vulnerabilities are emerging. One such vulnerability is prompt injection, a method that malicious actors can exploit to manipulate AI systems. Typically, the impact of prompt injection attacks is closely tied to the permissions granted to the AI. https://www.trendmicro.com/en_us/research/24/l/genai-prompt-injection-attack-threat.html

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

ATTACKS, BREACHES & LEAKS

- ***Lazarus Apt Targeted Employees At An Unnamed Nuclear-Related Organization*** **-** Kaspersky researchers observed the North Korea-linked Lazarus Group targeting at least two employees associated with the same nuclear-related organization over the course of one month. https://securityaffairs.com/172221/apt/lazarus-apt-targeted-employees-unnamed-nuclear-related-org.html
- ***Investigation Underway After Pittsburgh Regional Transit Alerts Riders Of Cybersecurity Incident*** - Pittsburgh Regional Transit is alerting riders after a ransomware attack was detected Thursday. In a statement Monday, PRT said an investigation has been launched to determine if any information has been compromised. https://www.wtae.com/article/pittsburgh-regional-transit-alerts-cybersecurity-attack/63268341
- ***Circle Electric Data Breach*** **-** Carsbeat is a digital platform for buying and selling new and used spare parts and used cars in the United Arab Emirates. https://www.breachsense.com/breaches/carsbeat-data-breach/
- ***Cicada3301 Ransomware Claims Attack on French Peugeot Dealership*** - Cicada3301, a ransomware group, has claimed responsibility for a data breach targeting Concession Peugeot (concessions.peugeot.fr), a prominent French automotive dealership linked to the Peugeot brand. The group claims to have stolen 35GB of sensitive data, marking a continuation of their aggressive cyber campaigns. https://hackread.com/cicada3301-ransomware-french-peugeot-dealership/
- ***Tracker firm Hapn spilled names of thousands of GPS tracking customers*** - GPS tracking firm Hapn exposed the names of thousands of its customers due to a website bug, TechCrunch has learned. https://techcrunch.com/2024/12/18/tracker-firm-hapn-spilling-names-of-thousands-of-gps-tracking-customers/

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

SECURITY VULNERABILITIES, ALERTS, ADVISORIES, & UPDATES

FEDORA SECURITY ADVISORIES

1. Sympa - https://lwn.net/Articles/1003540

DEBIAN SECURITY ADVISORIES

1. Xen - https://lists.debian.org/debian-security-announce/2024/msg00252.html
2. Fastnetmon - https://lists.debian.org/debian-security-announce/2024/msg00253.html

CHECK POINT SECURITY ADVISORIES

1. Ivanti - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-1172.html
2. DigiEver - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-1183.html
3. LibreNMS - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-1177.html
4. Fortinet - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2023-1610.html
5. Apple - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2023-1959.html
6. Apache - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-1164.html
7. Zabbix - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-1178.html
8. PHP - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-1189.html
9. EyesOfNetwork - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2020-4220.html
10. GeoServer - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-0559.html

ORACLE LINUX SECURITY UPDATE

1. Postgresql - https://lwn.net/Articles/1003541