Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

Daily Open-Source Cyber Report

December 13, 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

- Europol Takes Down Criminal Data Hub Manson Market In Busy Month For Law Enforcement
- Study Shows Potentially Higher Prevalence Of Spyware Infections Than Previously Thought
- Motive Uses AI to Tackle Fuel Fraud
- Pro-Russian Hacktivist Group Claims 6600 Attacks Targeting Europe
- A Hardwired Tsa Looks To The Future With 5g Implementation
- Connected Trucks Cybersecurity Key Growth Opportunities Report 2024-2029 - Managed Cybersecurity Services Will Gain Popularity among Commercial Vehicle Original Equipment Manufacturers
- HR And IT Are Among Top-Clicked Phishing Subjects

Emerging Threats & Vulnerabilities

- “aiocpa” Python Package Exposed as Cryptocurrency Infostealer
- ANEL and NOOPDOOR Backdoors Weaponized in New MirrorFace Campaign Against Japan
- MOONSHINE Exploit Kit and DarkNimbus Backdoor Enabling Earth Minotaur’s Multi-Platform Attacks
- Russian-linked Turla caught using Pakistani APT infrastructure for espionage
- Bootloader Vulnerability Impacts Over 100 Cisco Switches

Attacks, Breaches, & Leaks

- Bitcoin ATM Giant Byte Federal Hit by Hackers, 58,000 Users Impacted
- RansomHub Ransomware Attack on Shapes Precision Manufacturing
- No Need To Hack When It’s Leaking, Canadian Edition: Care1
- Japanese Publisher Paid $3 Million To Hacker Group After Cyberattack

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

EXECUTIVE NEWS

Europol Takes Down Criminal Data Hub Manson Market In Busy Month For Law Enforcement
Malwarebytes, 12/6/2024

A coordinated action between several European law enforcement agencies shut down an online marketplace called Manson Market that sold stolen data to any interested cybercriminal. What made this market attractive for cybercriminals was that they could buy data sorted by region and account balance with advanced filtering options. This allowed the criminals to carry out targeted fraud with greater efficiency. The law enforcement investigation started in 2022 when investigators were able to track very specific information used by scammers to the specialized marketplace. The scammers participated in fraudulent phone calls in which they impersonated bank employees to extract sensitive information, such as addresses and security answers, from their victims. https://www.malwarebytes.com/blog/news/2024/12/marketplace-serving-fraudsters-taken-down-by-european-law-enforcement

Study Shows Potentially Higher Prevalence Of Spyware Infections Than Previously Thought
Cyber Scoop, 12/4/2024

High-powered spyware might be more prevalent on victims' phones than commonly believed, research out Wednesday from iVerify suggests. Devices that the mobile device security firm's tech scanned found seven Pegasus spyware infections among 2,500 users who volunteered to participate in its investigation with a $0.99 version of its tech as an app. "Our investigation detected 2.5 infected devices per 1,000 scans — a rate significantly higher than any previously published reports," iVerify said in a blog post. Even with the caveat that its users — and those who self-selected to participate in the investigation — are from a population more likely to be targeted for spyware infections, that still was a startling rate, said Rocky Cole, chief operating officer and co-founder of the company. https://cyberscoop.com/study-shows-potentially-higher-prevalence-of-spyware-infections-than-previously-thought/

Motive Uses AI to Tackle Fuel Fraud
Fleet Owner, 12/9/2024

Motive recently announced new AI-powered fraud controls that detect fraud before it happens. Motive's new fraud control features identified more than $250,000 from more than 1,200 unauthorized transactions in a 30-day trial. According to the company, the Motive Card is the only fuel card that is fully integrated into a fleet management platform. The new fraud controls integrate telematics data from the Motive platform to give fleet managers the data and controls they need to identify and decline fraud transactions. https://www.fleetowner.com/technology/article/55248008/motive-card-introduces-ai-powered-fraud-controls-to-prevent-fuel-theft

Pro-Russian Hacktivist Group Claims 6600 Attacks Targeting Europe
Infosecurity Magazine, 12/5/2024

Pro-Russian hacktivist gang Noname has claimed over 6600 attacks since August 2022, almost exclusively targeting European nations, new research from Orange Cyberdefense has shown. The cybersecurity vendor’s Security Navigator 2025 report found that 96% of Noname’s attacks targets included Ukraine, Czech Republic, Spain, Poland and Italy and have been ongoing since Russia began its invasion of Ukraine in early 2022. The hacktivist group has not targeted the US once during this period, the researchers found. https://www.infosecurity-magazine.com/news/pro-russian-hacktivist-attacks/

A Hardwired TSA Looks To The Future With 5g Implementation
Federal News Network, 12/10/2024

The Transportation Security Administration has a mission to protect the nation’s transportation systems and ensure the movement of people and commerce. That mission comes with a portfolio of airports and other sites, and the responsibility to secure its networks while providing reliable network connectivity at all locations under TSA’s responsibility. At TSA, most of their critical network infrastructure is hardwired. That includes checkpoint equipment and computers operated by the Transportation Safety Officers. Hardwiring provides a level of security that wireless connectivity has been slower to match. But as the agency looks to the future, TSA is moving in the direction of exploring 5G technology implementation. https://federalnewsnetwork.com/technology-main/2024/12/a-hardwired-tsa-looks-to-the-future-with-5g-implementation/?readmore=1

Connected Trucks Cybersecurity Key Growth Opportunities Report 2024-2029 - Managed Cybersecurity Services Will Gain Popularity among Commercial Vehicle Original Equipment Manufacturers
Globe Newswire, 12/9/2024

The "Growth Opportunities in Connected Trucks Cybersecurity, Global, 2024-2029" report has been added to ResearchAndMarkets.com's offering. This analysis aims to examine the connected truck cybersecurity market, which includes light, medium, and heavy-duty vehicles. This analysis has a global scope, focusing on key regions - North America, Europe, China, India, and Japan - which it considers for market forecasting. With upcoming regulatory mandates, original equipment manufacturers (OEMs) must prioritize cybersecurity needs. Commercial vehicle OEMs are exploring partnerships with specialist companies to seamlessly adapt to the industry's best practices and ensure compliance with regulations. https://www.globenewswire.com/news-release/2024/12/09/2993588/0/en/Connected-Trucks-Cybersecurity-Key-Growth-Opportunities-Report-2024-2029-Managed-Cybersecurity-Services-Will-Gain-Popularity-among-Commercial-Vehicle-Original-Equipment-Manufacture.html

HR And IT Are Among Top-Clicked Phishing Subjects
The Cyber Express, 12/6/2024

A new report reveals that HR and IT-related phishing emails claim a significant 48.6 percent share of top-clicked phishing types globally. The research from KnowBe4 also shows that among large companies -- 1,000+ employees -- the most targeted industries are healthcare and pharmaceuticals with a Phish-Prone Percentage (PPP) of 51.4 percent, insurance on 48.8 percent and energy and utilities on 47.8 percent. Medium businesses see hospitality move into the top spot with a PPP of 39.7 percent, healthcare and pharmaceuticals on 38.8 percent and the consulting industry in the top three for the first time with a PPP of 36.2 percent. Smaller firms with under 250 staff again have healthcare and pharma at the number one spot, with a PPP of 34.7 percent. Education is second on 32.4 percent, slightly more than one point more lower than the previous year, with hospitality third on a PPP of 31.2 percent.
https://betanews.com/2024/12/03/hr-and-it-are-among-top-clicked-phishing-subjects/

TECHNICAL SUMMARY

EMERGING THREATS & EXPLOITS

- ***"aiocpa" Python Package Exposed as Cryptocurrency Infostealer -*** The machine learning-based threat-hunting system of leading threat intelligence and cybersecurity firm ReversingLabs (RL) recently detected malicious code in a legitimate-looking package, "aiocpa." According to RL's investigation, shared with Hackread.com, this package was designed to compromise cryptocurrency wallets. https://hackread.com/aiocpa-python-package-cryptocurrency-infostealer/
- ***ANEL and NOOPDOOR Backdoors Weaponized in New MirrorFace Campaign Against Japan*** - The China-linked threat actor known as MirrorFace has been attributed to a new spear-phishing campaign mainly targeting individuals and organizations in Japan since June 2024. https://thehackernews.com/2024/12/anel-and-noopdoor-backdoors-weaponized.html
- ***MOONSHINE Exploit Kit and DarkNimbus Backdoor Enabling Earth Minotaur's Multi-Platform Attacks –*** We have been continuously monitoring the MOONSHINE exploit kit's activity since 2019. During our research, we discovered a MOONSHINE exploit kit server with improper operational security: Its server exposed MOONSHINE's toolkits and operation logs, which revealed the information of possible victims and the attack tactics of a threat actor we have named Earth Minotaur. https://www.trendmicro.com/en_us/research/24/l/earth-minotaur.html
- ***Russian-linked Turla caught using Pakistani APT infrastructure for espionage –*** A Russian cyber-espionage group with ties to the country's Federal Security Service has been caught using networks associated with a Pakistani-based APT group. This operation marks the fourth recorded incident since 2019 where the Russian group, known commonly as Turla, has embedded themselves within another threat actor's operations. https://cyberscoop.com/turla-infiltrates-pakistani-apt-networks-microsoft-lumen/
- ***Bootloader Vulnerability Impacts Over 100 Cisco Switches -*** Cisco on Wednesday announced patches for a vulnerability in the NX-OS software's bootloader that could allow attackers to bypass image signature verification. https://www.securityweek.com/bootloader-vulnerability-impacts-over-100-cisco-switches/

ATTACKS, BREACHES & LEAKS

- ***Bitcoin ATM Giant Byte Federal Hit by Hackers, 58,000 Users Impacted -*** Byte Federal, the US's largest Bitcoin ATM operator offering around 1,200 Bitcoin ATMs across the country, recently confirmed a data breach that potentially exposed the personal information of 58,000 customers. https://hackread.com/bitcoin-atm-byte-federal-hackers-users-impacted/
- ***RansomHub Ransomware Attack on Shapes Precision Manufacturing*** - Shapes Precision Manufacturing, a specialized manufacturer based in Palm Bay, Florida, has allegedly fallen victim to a ransomware attack by the notorious RansomHub group. The attack, discovered on December 2, reportedly compromised approximately 500GB of sensitive data, now claimed to be available on RansomHub's dark web platform. https://www.halcyon.ai/attacks/ransomhub-ransomware-strikes-shapes-precision-manufacturing-6ad47
- ***No Need To Hack When It's Leaking, Canadian Edition: Care1 -*** Jeremiah Fowler discovered a non-password-protected database that contained more than 4.8 million records belonging to Care1 — a Canadian company offering AI software solutions to support optometrists in delivering enhanced patient care: https://databreaches.net/2024/12/12/no-need-to-hack-when-its-leaking-canadian-edition-care1/
- ***Japanese Publisher Paid $3 Million To Hacker Group After Cyberattack*** - A Russia-linked hacking group e-mailed multiple executives of Japanese publisher Kadokawa Corp. that it had received $2.98 million in cryptocurrency from the firm after it was hit by a massive cyberattack in June, a company source said Thursday. https://english.kyodonews.net/news/2024/12/fffebe5585f1-japanese-publisher-paid-3-million-to-hacker-group-after-cyberattack.html

SECURITY VULNERABILITIES, ALERTS, ADVISORIES, & UPDATES

SUSE Security Updates

1. go1.23-openssl - https://www.suse.com/support/update/announcement/2024/suse-ru-20244307-1
2. hawk2 - https://www.suse.com/support/update/announcement/2024/suse-ru-20244309-1
3. nvidia-open-driver-G06-signed - https://www.suse.com/support/update/announcement/2024/suse-ru-20244310-1
4. iputils - https://www.suse.com/support/update/announcement/2024/suse-ru-20244311-1
5. fence-agents - https://www.suse.com/support/update/announcement/2024/suse-ru-20244312-1

Fedora Security Advisories

1. chromium - https://lwn.net/Articles/1002014
2. linux-firmware - https://lwn.net/Articles/1002015
3. matrix-synapse –
   a. https://lwn.net/Articles/1002016
   b. https://lwn.net/Articles/1002017

Red Hat Security Advisories

1. python3.12 - https://access.redhat.com/errata/RHSA-2024:11035

Zero Day Initiative Advisories & Updates

1. linux kernel - https://www.zerodayinitiative.com/advisories/ZDI-24-1688/
2. Progress Software - https://www.zerodayinitiative.com/advisories/ZDI-24-1687/

***** FAIR USE NOTICE*****

This message contains copyrighted material whose use has not been specifically authorized by the copyright owner. The ST-ISAC is making it available to ISAC members who have expressed a prior interest in receiving information to advance their understanding of threat activities in the interest of protecting the national infrastructure of the United States. We believe that this constitutes a 'fair use' of the copyrighted material as provided for in section 107 of the U.S. Copyright Law. If you wish to use this copyrighted material for purposes of your own that go beyond 'fair use,' you must obtain permission from the copyright owner.