Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

Daily Open-Source Cyber Report

December 6, 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

- U.S. Citizen Sentenced for Spying on Behalf of China's Intelligence Agency
- Federal Transportation Officials Aim To 'bridge Gaps' In OT Cybersecurity
- 'Operation Undercut' Adds to Russia Malign Influence Campaigns
- Supply Chain Managers Underestimate Cybersecurity Risks In Warehouses
- SmokeLoader Malware Campaign Targets Companies in Taiwan
- The Phishing Threat Landscape Evolves
- APT Trends Report Q3 2024

Emerging Threats & Vulnerabilities

- Hackers Exploit Docker Remote API Servers To Inject Gafgyt Malware
- Cybercriminals Exploit Popular Game Engine Godot to Distribute Cross-Platform Malware
- New Android Spyware Found On Phone Seized By Russian FSB
- Printer Problems? Beware The Bogus Help
- Microsoft Patches Exploited Vulnerability in Partner Network Website

Attacks, Breaches, & Leaks

- Max Trans Data Breach
- Ransomware Group Ransomhub Hits: hanwhacimarron.com
- Deloitte Hacked – Brain Cipher Ransomware Group Allegedly Stolen 1 TB of Data
- Express Services Disclosed A Data Breach. One Month Later, They Learned They Had A Second Data Security Problem.
- Romania's Election Systems Targeted In Over 85,000 Cyberattacks

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

EXECUTIVE NEWS

U.S. Citizen Sentenced for Spying on Behalf of China's Intelligence Agency
The Hacker News, 11/29/2024

A 59-year-old U.S. citizen who immigrated from the People's Republic of China (PRC) has been sentenced to four years in prison for conspiring to act as a spy for the country and sharing sensitive information about his employer with China's principal civilian intelligence agency. Ping Li, 59, of Wesley Chapel, Florida, is said to have served as a cooperative contact for the Ministry of State Security (MSS) as early as August 2012, working at their behest to obtain information that's of interest to the Chinese government. Li was employed at telecom giant Verizon and later at information technology service company Infosys. https://thehackernews.com/2024/11/us-citizen-sentenced-for-spying-on.html

Federal Transportation Officials Aim To 'bridge Gaps' In OT Cybersecurity
Cyber Scoopl, 12/4/2024

From supporting aircraft systems to ensuring railway signals don't falter, the operational technology that underpins transportation networks across the country is critical to daily life — and highly vulnerable to threats. For Katherine Rawls, director of sector cyber engagement at the Department of Transportation, acknowledging that reality sparks various debates on how to meet those challenges head on. "We're talking about preserving the safety and reliability of OT systems that millions rely on daily," Rawls said. "So we're focused on, how do we integrate cybersecurity into all hazards safety management systems? How do we bridge gaps … between the cybersecurity and safety community?" https://cyberscoop.com/operational-technology-cybersecurity-challenges-collaboration-strategies-department-of-transportation/

'Operation Undercut' Adds to Russia Malign Influence Campaigns
Dark Reading, 11/27/2024

Social Design Agency (SDA,) a Russian outfit the US government recently accused of operating a malign influence campaign dubbed "Doppelgänger," is running another similar campaign concurrently, targeting audiences in the US, Ukraine, and Europe. The primary objective of the SDA's "Operation Undercut" campaign, much like Doppelgänger, is to erode support for Ukraine in its war with Russia. However, the campaign also extends its interference to other areas, including the ongoing Middle East conflict, internal EU politics, and matters related to the 2024 US presidential election https://www.darkreading.com/cybersecurity-operations/operation-undercut-russia-malign-influence-campaigns

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

Supply Chain Managers Underestimate Cybersecurity Risks In Warehouses
Help Net Security, 11/27/2024

As the backbone of the supply chain, a cyberattack on a warehouse can result in major consequences such as significant operational downtime, damage to a company's reputation and financial losses. Given the vast amount of data warehouses possess, hackers may also obtain access to sensitive customer information, impacting trust and loyalty. Despite these risks, according to supply chain managers, cybersecurity is a top concern for only 58% of warehouses, while 13% do not view it as a concern at all. "The supply chain industry has been slow to adapt to the evolving cybersecurity landscape. With the rise of warehouse modernization, the proliferation of IoT devices and the growing rate of cybercriminals targeting this industry, the risk of damaging cyberattacks has significantly increased. https://www.helpnetsecurity.com/2024/11/27/warehouses-cybersecurity-concern/

SmokeLoader Malware Campaign Targets Companies in Taiwan
Infosecurity Magazine, 12/2/2024

A sophisticated malware campaign leveraging SmokeLoader has been observed targeting Taiwanese companies across manufacturing, healthcare and IT sectors. SmokeLoader, a modular malware known for its adaptability and evasion techniques, is being used in this attack to directly execute its payloads rather than serving as a downloader for other malicious software. Identified by FortiGuard Labs, the campaign begins with phishing emails designed to trick recipients into opening malicious attachments. These emails, written in local languages and featuring copied text for authenticity, often include subtle formatting inconsistencies that could signal their fraudulent nature. https://www.infosecurity-magazine.com/news/smokeloader-malware-taiwan/

The Phishing Threat Landscape Evolves
Engineer Live, 11/25/2024

Phishing is on the rise. Egress' latest Phishing Threat Trends Report shows a 28 percent surge in attacks in the second quarter of 2024 alone. But what's behind the increase? There are a few factors in play. Like any other form of threat, phishing is becoming more sophisticated with hackers now having access to a variety of new AI-powered tools to generate email messages, payloads, and even deepfakes. Further, these technologies and the cyberattacks they can create are now easier to access than ever. Especially as more hackers tap into the professional services on offer from a mature and diverse Crime as a Service (CaaS) ecosystem of providers selling everything from the mechanisms to create attacks to pre-packaged phishing toolkits that promise to evade native defenses and secure email gateways (SEGs). https://betanews.com/2024/11/28/the-phishing-threat-landscape-evolves/

APT Trends Report Q3 2024
The Hacker News, 11/25/2024

Kaspersky's Global Research and Analysis Team (GReAT) has been releasing quarterly summaries of advanced persistent threat (APT) activity for over seven years now. Based on our threat intelligence research, these summaries offer a representative overview of what we've published and discussed in more detail in our private APT reports. They are intended to highlight the significant events and findings that we think are important for people to know about. This is our latest roundup, covering activity we observed during Q3 2024. In the second half of 2022, a wave of attacks from an unknown threat actor targeted victims with a new type of attack framework that we dubbed P8. The campaign targeted Vietnamese victims, mostly from the financial sector, with some from the real estate sector.
https://securelist.com/apt-report-q3-2024/114623/

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

TECHNICAL SUMMARY

EMERGING THREATS & EXPLOITS

- ***Hackers Exploit Docker Remote API Servers To Inject Gafgyt Malware -*** The Gafgyt malware (often referred to as Bashlite or Lizkebab) has expanded its attack scope by targeting publicly exposed Docker Remote API servers. https://cybersecuritynews.com/gafgyt-malware-attacks-docker-api-servers/
- ***Cybercriminals Exploit Popular Game Engine Godot to Distribute Cross-Platform Malware*** - After a Russian programmer was detained by Russia's Federal Security Service (FSB) for fifteen days and his phone confiscated, it was discovered that a new spyware was secretly installed on his device upon its return. https://thehackernews.com/2024/11/cybercriminals-exploit-popular-game.html
- ***New Android Spyware Found On Phone Seized By Russian FSB –*** The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Monday added a now-patched critical security flaw impacting Array Networks AG and vxAG secure access gateways to its Known Exploited Vulnerabilities (KEV) catalog following reports of active exploitation in the wild. https://thehackernews.com/2024/11/cisa-urges-agencies-to-patch-critical.html
- ***Printer Problems? Beware The Bogus Help –*** Anyone who has ever used a printer likely has had a frustrating experience at some point. There always seems to be some kind of issue with the software not responding, paper getting jammed or one of many other possible failures. https://www.malwarebytes.com/blog/scams/2024/11/printer-problems-beware-the-bogus-help
- ***Microsoft Patches Exploited Vulnerability in Partner Network Website -*** The tech giant has patched vulnerabilities in Azure, Copilot Studio, and its Partner Network website — one security hole in each — but customers do not need to take any action. CVE identifiers and advisories have been published for transparency only. https://www.securityweek.com/microsoft-patches-exploited-vulnerability-in-partner-network-website/

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

ATTACKS, BREACHES & LEAKS

- ***Max Trans Data Breach*** **-** Max Trans is a locally owned trucking company based in Humboldt, TN, dedicated to providing superior logistics solutions with a focus on safety, efficiency, and customer satisfaction. https://www.halcyon.ai/attacks/ransomhub-hits-belgian-manufacturer-potteau-in-data-breach
- ***Ransomware Group Ransomhub Hits: hanwhacimarron.com*** - A ransomware attack disrupted the operations of a major energy industry contractor, ENGlobal Corporation. Founded in 1985, ENGlobal Corporation designs automated control systems for commercial and government sectors, reporting $6 million in Q3 revenue and $18.4 million year-to-date.https://www.infosecurity-magazine.com/news/tmobile-salt-typhoon-did-not/
- ***Deloitte Hacked – Brain Cipher Ransomware Group Allegedly Stolen 1 TB of Data*** **-** Notorious ransomware group Brain Cipher has claimed to have breached Deloitte UK, allegedly exfiltrating over 1 terabyte of sensitive data from the professional services giant. https://cybersecuritynews.com/deloitte-hacked/
- ***Express Services Disclosed A Data Breach. One Month Later, They Learned They Had A Second Data Security Problem.*** - Express Employment Professionals ("Express Pros") describes itself as a leading staffing agency in the U.S., "specializing in matching job seekers with the best jobs for their skills and experience." Express Pros is the flagship brand for Express Services and conducts business across the U.S., Canada, South Africa, Australia, and New Zealand. Express Pros operates as a franchise. https://databreaches.net/2024/12/04/express-services-disclosed-a-data-breach-one-month-later-they-learned-they-had-a-second-data-security-problem/
- ***Romania's Election Systems Targeted In Over 85,000 Cyberattacks*** **-** A declassified report from Romania's Intelligence Service says that the country's election infrastructure was targeted by more than 85,000 cyberattacks. https://www.bleepingcomputer.com/news/security/romanias-election-systems-targeted-in-over-85-000-cyberattacks/

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

SECURITY VULNERABILITIES, ALERTS, ADVISORIES, & UPDATES

SUSE Security Updates

1. MozillaFirefox - https://www.suse.com/support/update/announcement/2024/suse-su-20244253-1
2. java-1_8_0-ibm - https://www.suse.com/support/update/announcement/2024/suse-su-20244252-1
3. 389-ds - https://www.suse.com/support/update/announcement/2024/suse-ru-20244245-1
4. shared-mime-info - https://www.suse.com/support/update/announcement/2024/suse-ru-20244244-1

Fedora Security Advisories

1. pam - https://lwn.net/Articles/1001141

Mageia Security Advisories

1. Kubernetes - http://advisories.mageia.org/MGASA-2024-0389.html

Zero Day Initiative Advisories & Updates

1. iXsystems –
    a. https://www.zerodayinitiative.com/advisories/ZDI-24-1643/
    b. https://www.zerodayinitiative.com/advisories/ZDI-24-1644/
2. Progress Software WhatsUp - https://www.zerodayinitiative.com/advisories/ZDI-24-1645/

Other

1. Google Chrome –
    a. https://chromereleases.googleblog.com/2024/12/chrome-beta-for-ios-update.html
    b. https://chromereleases.googleblog.com/2024/12/chrome-stable-for-ios-update_6.html