Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

Daily Open-Source Cyber Report

December 24, 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 Issues Updated Draft Of National Cyber Incident Response Plan
- Israeli Court To Hear U.S. Extradition Request For Alleged Lockbit Developer
- Tp-Link Faces U.S. National Security Probe, Potential Ban On Devices
- Navigating the Road Ahead: How AI and Vehicle Automation are Transforming the Transportation Industry
- Attackers Can Find New APIs in 29 Seconds: Wallarm
- Overlooking Platform Security Weakens Long-Term Cybersecurity Posture
- Logistics Technology Trends to Watch in 2025

Emerging Threats & Vulnerabilities

- 'fix It' Social-Engineering Scheme Impersonates Several Brands
- New Glutton Malware Exploits Popular PHP Frameworks Like Laravel and ThinkPHP
- MUT-1244 Targeting Security Researchers, Red Teamers, And Threat Actors
- PUMAKIT, A Sophisticated Rootkit That Uses Advanced Stealth Mechanisms
- Fake Captcha Campaign Highlights Risks of Malvertising Networks

Attacks, Breaches, & Leaks

- Bright Bolt Enterprises Data Breach
- KillSec Ransomware Targets JSSR Options in Thailand
- Illinois Department Of Human Services Shares Info On Incident Involving Protected Personal Information
- LastPass breach comes back to haunt users as hackers steal $12 million in two days
- Ascension Cyberattack Exposed Personal Data Of 5.6 Million People, Including Wisconsin Patients

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

EXECUTIVE NEWS

CISA Issues Updated Draft Of National Cyber Incident Response Plan
Next Gov, 12/16/2024

America's top cyber agency is out with an updated blueprint to help federal government entities and their private sector counterparts respond accordingly in the event of a cyberattack that severely cripples the economy and society. The Cybersecurity and Infrastructure Security Agency released the updated National Cyber Incident Response Plan into the Federal Register on Monday, inviting the public to comment on it over the next month. The drafted plan outlines four tiers — asset response, threat response, intelligence support and affected entity response — as a means of planning ahead for unlikely but potentially destructive cyberattacks that could be launched by foreign adversaries against critical U.S. infrastructure like banks, railways, electric grids and water treatment plants.
https://www.nextgov.com/cybersecurity/2024/12/cisa-issues-updated-draft-national-cyber-incident-response-plan/401687/

Israeli Court To Hear U.S. Extradition Request For Alleged Lockbit Developer
Cyber Scoop, 12/19/2024

An Israeli Court is set to deliberate a significant extradition case involving Rostislav Panev, an Israeli citizen alleged to be involved with the notorious LockBit ransomware gang. According to Israeli news outlet Ynet, a U.S. extradition request was made public Thursday claiming that between 2019 and 2024, Panev served as a software developer for LockBit. During this period, LockBit is alleged to have executed cyberattacks impacting roughly 2,500 victims globally, including U.S. governmental and health care organizations. The U.S. Department of Justice places LockBit among the most detrimental ransomware groups in operation, responsible for financial losses exceeding $500 million.
https://cyberscoop.com/rostislav-panev-lockbit-israel-extradition/

TP-Link Faces U.S. National Security Probe, Potential Ban On Devices
Malwarebytes Labs, 12/19/2024

The US government launched a national security investigation into the popular, Chinese-owned router maker TP-Link, with a potential eye on banning the company's devices in the United States. The investigation comes amid heightened tension between the US and the Chinese government, and after a public letter from members of the US House of Representatives this summer that alleged that TP-Link was engaged in predatory pricing practices, driven by ulterior motives, and possibly sponsored by China. US officials noted how TP-Link undercut the competition on price to become the market leader for Small Office/Home Office (SOHO) network appliances. https://www.malwarebytes.com/blog/news/2024/12/tp-link-faces-us-national-security-probe-potential-ban-on-devices

Navigating the Road Ahead: How AI and Vehicle Automation are Transforming the Transportation Industry
Foley, 12/17/2024

Artificial Intelligence (AI) is expected to impact almost every modern industry, with no exception for the automotive and transportation industries. Today's cars are more "connected" than ever, offering features such as real-time traffic updates, vehicle-to-vehicle (V2V) and vehicle-to-everything (V2X) communication, predictive maintenance reminders, and advanced driver assistance system (ADAS) features like lane-keep assist and automated emergency braking. With a seemingly unrelenting focus across all industries to become AI leaders, it's only a matter of time until the 20th century's fanciful notion of full vehicle automation becomes a 21st century reality.
https://www.foley.com/insights/publications/2024/12/ai-vehicle-automation-transforming-transportation-industry/

Attackers Can Find New APIs in 29 Seconds: Wallarm
Security Boulevard, 12/17/2024

As APIs have become a cornerstone of modern business, they also are increasingly becoming a favorite target of threat actors looking to gain initial access to sensitive data or to disrupt services. A report this week by API security vendor Wallarm illustrates just how aggressive the hackers are. Wallarm, using an API honeypot to attract attackers, found that it took bad actors an average of 29 seconds to discover a newly deployed API and under a minute to exploit an unprotect API. The vendor also found that APIs have overtaken web applications as targets of attacks. The San Francisco-based company launched its honeypot in November and researchers were so startled by the results that they issued their first report after only 20 days of activity. https://securityboulevard.com/2024/12/attackers-can-find-new-apis-in-29-seconds-wallarm/

Overlooking Platform Security Weakens Long-Term Cybersecurity Posture
Help Net Security, 12/15/2024

The report, based on a global study of 800+ IT and security decision-makers (ITSDMs) and 6000+ work-from-anywhere (WFA) employees, shows that platform security is a growing concern with 81% of ITSDMs agreeing that hardware and firmware security must become a priority to ensure attackers cannot exploit vulnerable devices. However, 68% report that investment in hardware and firmware security is often overlooked in the total cost of ownership (TCO) for devices. This is leading to costly security headaches, management overheads and inefficiencies further down the line.
https://www.helpnetsecurity.com/2024/12/16/platform-security-concerns/

Logistics Technology Trends to Watch in 2025
Dark Reading, 12/11/2024

As we look toward 2025, one thing is clear: the supply chain volatility of recent years isn't going anywhere. The continued need for adaptable, resilient strategies will remain critical for success. How will logistics leaders leverage technology to improve global freight networks, anticipate disruptions, navigate new trade policies, and boost reliability in an increasingly turbulent supply chain environment? Here are trends that will advance today's digital logistics operations. Continuing to integrate global logistics and supply chain systems will revolutionize operational performance, strategic planning, and efficiency. Additionally, by connecting real-time data, predictive analytics, and data insights, users will accelerate resiliency, response times, and adaptability, enabling companies to tackle challenges quickly and streamline operations. https://www.globaltrademag.com/logistics-technology-trends-to-watch-in-2025/

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

TECHNICAL SUMMARY

EMERGING THREATS & EXPLOITS

- ***'fix It' Social-Engineering Scheme Impersonates Several Brands*** **-** More and more, threat actors are leveraging the browser to deliver malware in ways that can evade detection from antivirus programs. Social engineering is a core part of these schemes and the tricks we see are sometimes very clever. https://www.malwarebytes.com/blog/news/2024/12/fix-it-social-engineering-scheme-impersonates-several-brands
- ***New Glutton Malware Exploits Popular PHP Frameworks Like Laravel and ThinkPHP*** - Cybersecurity researchers have discovered a new PHP-based backdoor called Glutton that has been put to use in cyber attacks targeting China, the United States, Cambodia, Pakistan, and South Africa. https://thehackernews.com/2024/12/new-glutton-malware-exploits-popular.html
- ***MUT-1244 Targeting Security Researchers, Red Teamers, And Threat Actors*** **-** A threat actor tracked as MUT-1244 by DataDog researchers has been targeting academics, pentesters, red teamers, security researchers, as well as other threat actors, in order to steal AWS access keys, WordPress account credentials and other sensitive data. https://www.helpnetsecurity.com/2024/12/16/mut-1244-targeting-security-researchers-threat-aws-wordpress-data-theft/
- ***PUMAKIT, A Sophisticated Rootkit That Uses Advanced Stealth Mechanisms*** **–** Elastic Security Lab researchers discovered a new loadable kernel module (LKM) rootkit called PUMAKIT that supports advanced evasion mechanisms. https://securityaffairs.com/172016/malware/pumakit-sophisticated-rootkit.html
- ***Fake Captcha Campaign Highlights Risks of Malvertising Networks*** **–** A new large-scale campaign distributing Lumma infostealer malware through fake captcha pages has been observed using malvertising to exploit weaknesses in the digital advertising ecosystem. The attacks exposed thousands of victims to credential theft and financial losses. https://www.infosecurity-magazine.com/news/fake-captcha-campaign-risks/

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

ATTACKS, BREACHES & LEAKS

- ***Bright Bolt Enterprises Data Breach -*** Bright Bolt Enterprises is a leading supplier of tools, fasteners, personal protective equipment, and construction supplies for industrial and construction companies. . https://www.breachsense.com/breaches/bright-bolt-enterprises-data-breach/
- ***KillSec Ransomware Targets JSSR Options in Thailand*** - JSSR Options Co., Ltd., a key player in Thailand's transportation and logistics sector, has recently fallen victim to a ransomware attack by the notorious KillSec group. This incident underscores the vulnerabilities faced by companies in the digital age, particularly those involved in high-value transactions and logistics operations. https://www.halcyon.ai/attacks/killsec-ransomware-targets-jssr-options-in-thailand
- ***Illinois Department Of Human Services Shares Info On Incident Involving Protected Personal Information -*** On April 25, 2024, IDHS experienced a privacy breach. An outside entity, through a phishing campaign, gained access to multiple employee accounts, and files associated with the accounts. The files included the Social Security numbers (SSNs) of 4,701 customers and three employees. https://www.effinghamradio.com/2024/12/20/illinois-department-of-human-services-shares-info-on-incident-involving-protected-personal-information/
- ***Lastpass Breach Comes Back To Haunt Users As Hackers Steal $12 Million In Two Days*** - A major data breach at password manager firm LastPass in 2022 is still causing mayhem two years later, with cyber criminals using stolen information to carry out further attacks. https://databreaches.net/2024/12/18/lastpass-breach-comes-back-to-haunt-users-as-hackers-steal-12-million-in-two-days/
- ***Ascension Cyberattack Exposed Personal Data Of 5.6 Million People, Including Wisconsin Patients*** - Nearly 5.6 million people were affected in the ransomware attack that hit Ascension in May, the national health system now says. https://www.msn.com/en-us/health/other/ascension-cyberattack-exposed-personal-data-of-5-6-million-people-including-wisconsin-patients/ar-AA1wgNal

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

SECURITY VULNERABILITIES, ALERTS, ADVISORIES, & UPDATES

SUSE Security Updates

1. Vhostmd - https://www.suse.com/support/update/announcement/2024/suse-su-20244416-1
2. resource-agents –
    a. https://www.suse.com/support/update/announcement/2024/suse-ru-20244417-1
    b. https://www.suse.com/support/update/announcement/2024/suse-ru-20244418-1
    c. https://www.suse.com/support/update/announcement/2024/suse-ru-20244419-1
    d. https://www.suse.com/support/update/announcement/2024/suse-ru-20244420-1
3. Poppler –
    a. https://www.suse.com/support/update/announcement/2024/suse-su-20244421-1
    b. https://www.suse.com/support/update/announcement/2024/suse-su-20244422-1

Fedora Security Advisories

1. python3-docs - https://lwn.net/Articles/1003371
2. python3.12 - https://lwn.net/Articles/1003372

Mageia Security Advisories

1. emacs - http://advisories.mageia.org/MGASA-2024-0397.html

Check Point Security Advisories

1. Craft - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-1184.html
2. Dahua Security - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2021-2137.html
3. VMware - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-1176.html

Other

1. Adobe - https://helpx.adobe.com/security/products/coldfusion/apsb24-107.html
2. Google - https://chromereleases.googleblog.com/2024/12/stable-channel-update-for-chromeos_23.html

email st-isac@surfacetransportationisac.org