Information Sharing &
Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

Daily Open-Source Cyber Report

November 22, 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

Securing Public Gatherings (SPG)

Public gatherings are increasingly vulnerable to violent attacks and criminal activity because of their relative accessibility and large number of potential targets. The Cybersecurity & Infrastructure Security Agency (CISA) provides a compendium of resources to help mitigate potential risks to these events and spaces in today's dynamic and rapidly evolving threat environment. The resources cover the numerous threat vectors in CISA's portfolio, including unauthorized access to facilities, cybersecurity, election security, active shooters, bombings, and small unmanned aircraft systems (sUAS).
https://www.cisa.gov/securing-public-gatherings

Additional Resources:

- Mass Gatherings Action Guide: https://www.cisa.gov/sites/default/files/publications/Mass%20Gatherings%20-%20Security%20Awareness%20for%20ST-CP.PDF
- Securing Public Gatherings Postcard: https://www.cisa.gov/sites/default/files/publications/Securing%20Public%20Gatherings%20Postcard_508.pdf
- Suspicious or Unattended Item Postcard: https://www.cisa.gov/sites/default/files/publications/Unattended-vs-Suspicious-Postcard.pdf

Security Planning Workbook: https://www.cisa.gov/sites/default/files/2023-10/CISA_AASB_Security_Planning_Workbook_508_Compliant_20230929.pdf

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

AT-A-GLANCE

Executive News

- CISA and Partners Release Update to BianLian Ransomware Cybersecurity Advisory
- TSA Not Monitoring Transportation Sector Efforts To Stop Ransomware, Watchdog Says
- 20% of Industrial Manufacturers Are Using Network Security as a First Line of Defense
- Sitting Ducks DNS Attacks Put Global Domains at Risk
- Caterpillar Successfully Deploys Fully Autonomous Off-Highway Truck
- Stolen Vehicle Recovery Market To Reach $13.9 Bn By 2032, Says Global Market Insights Inc.
- 5 BCDR Oversights That Leave You Exposed to Ransomware

Emerging Threats & Vulnerabilities

- LightSpy Spyware Operation Expands to Windows
- High-Severity Flaw in PostgreSQL Allows Hackers to Exploit Environment Variables
- Palo Alto Networks Patches Critical Zero-Day Firewall Bug
- Fraud Network Uses 4,700 Fake Shopping Sites To Steal Credit Cards
- Critical Really Simple Security plugin flaw impacts 4M+ WordPress sites

Attacks, Breaches, & Leaks

- Interoute Hit By Lynx Ransomware: 50GB Data Compromised
- [QILIN] – Ransomware Victim: Stalcop Metal Forming LLC
- James H. Maloy Data Breach
- Hackers Redirect $250,000 Payment In Ilearningengines Cyberattack
- Mexico’s President Says Government Is Investigating Reported Ransomware Hack Of Legal Affairs Office

EXECUTIVE NEWS

CISA and Partners Release Update to BianLian Ransomware Cybersecurity Advisory
CISA, 11/20/2024

Today, CISA, the Federal Bureau of Investigation (FBI), and the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) released updates to #StopRansomware: BianLian Ransomware Group on observed tactics, techniques, and procedures (TTPs) and indicators of compromise attributed to data extortion group, BianLian. The advisory, originally published May 2023, has been updated with additional TTPs obtained through FBI and ASD's ACSC investigations and industry threat intelligence as of June 2024. BianLian is likely based in Russia, with Russia-based affiliates, and has affected organizations in multiple U.S. critical infrastructure sectors since June 2022. They have also targeted Australian critical infrastructure sectors, professional services, and property development. https://www.cisa.gov/news-events/alerts/2024/11/20/cisa-and-partners-release-update-bianlian-ransomware-cybersecurity-advisory

TSA Not Monitoring Transportation Sector Efforts To Stop Ransomware, Watchdog Says
The Record, 11/19/2024

Efforts by the Transportation Security Administration (TSA) to address cybersecurity issues faced significant criticism this week from government watchdogs, members of Congress and regulated companies. A U.S. Government Accountability Office (GAO) report on Tuesday said four of the six cybersecurity recommendations made to TSA since 2018 have still not been addressed — including one centered around the agency's efforts to protect companies from ransomware. "For example, in January 2024, GAO reported that ransomware was having increasingly devastating impacts in the sector and found that TSA's security directives did not align with ransomware leading practices," said Tina Won Sherman, director of Homeland Security and Justice at the GAO. https://therecord.media/tsa-not-monitoring-transportation-ransomware-efforts-hearing-gao

20% of Industrial Manufacturers Are Using Network Security as a First Line of Defense
Dark Reading, 11/13/2024

Industrial manufacturers ranked network security as their top cybersecurity investment to guard against adverse cyber events, according to a recent State of Technology in Manufacturing survey by global technology intelligence firm ABI Research. With increasingly connected and digitized industrial assets providing ever more information about processes and workforce, manufacturers are focusing their security on network security technologies such as authentication and access control. Coupled with a growing body of industrial-focused security regulation and an expanding cybercrime element (https://www.darkreading.com/ics-ot-security/20-of-industrial-manufacturers-are-using-network-security-as-a-first-line-of-defense

Sitting Ducks DNS Attacks Put Global Domains at Risk
Infosecurity Magazine, 11/14/2024

Over one million domains have been found to be potentially vulnerable to a "Sitting Ducks" attack, a cyber threat that exploits DNS misconfigurations to hijack domains. The report, published by Infoblox Threat Intel, suggests that this type of attack, active since 2018, allows threat actors to leverage hijacked domains for malicious activities ranging from malware distribution to phishing. The Domain Name System (DNS) is a crucial part of the Internet's infrastructure, acting as its "phonebook." It converts human-readable domain names, such as www.example.com, into machine-readable IP addresses, like 192.0.2.1. This translation allows users to access websites, applications, and online services without needing to remember complex numerical codes.
https://www.infosecurity-magazine.com/news/sitting-ducks-dns-attacks-global/

Caterpillar Successfully Deploys Fully Autonomous Off-Highway Truck
Canadian Mining, 11/20/2024

Caterpillar has successfully demonstrated the fully autonomous operation of its Cat 777 off-highway truck. The debut marks a significant milestone in Caterpillar's objective to deliver an autonomous hauling solution for the quarry and aggregates sector. This successful deployment highlights the progress being made between Caterpillar and Luck Stone, the largest producer of crushed stone, sand, and gravel in the United States. In December 2022, Luck Stone and Caterpillar announced an agreement to accelerate the development of Caterpillar's autonomous solutions for quarry and aggregate applications. https://security.googleblog.com/2024/11/retrofitting-spatial-safety-to-hundreds.html

Stolen Vehicle Recovery Market To Reach $13.9 Bn By 2032, Says Global Market Insights Inc.
GlobeNewswire 11/19/2024

The stolen vehicle recovery market valuation is predicted to exceed USD 13.9 billion by 2032, reported in a research analysis by Global Market Insights Inc. The increasing incidence of vehicle theft is a significant driver of this stolen vehicle recovery market demand. As theft methods become more sophisticated, there is a growing demand for advanced recovery solutions. Factors such as economic pressures, organized crime, and the high value of vehicle parts in the black market contribute to rising theft rates, particularly in urban areas where income inequality is prominent. The financial burden of vehicle theft on individuals and businesses highlights the urgent need for investment in recovery technologies. This situation prompts insurance companies, law enforcement agencies, and vehicle owners to seek more effective solutions to tackle the issue. https://www.globenewswire.com/news-release/2024/11/19/2983463/0/en/Stolen-Vehicle-Recovery-Market-to-reach-13-9-Bn-by-2032-Says-Global-Market-Insights-Inc.html

5 BCDR Oversights That Leave You Exposed to Ransomware
The Hacker News, 11/14/2024

Ransomware isn't just a buzzword; it's one of the most dreaded challenges businesses face in this increasingly digitized world. Ransomware attacks are not only increasing in frequency but also in sophistication, with new ransomware groups constantly emerging. Their attack methods are evolving rapidly, becoming more dangerous and damaging than ever. Almost all respondents (99.8%) in a recent survey said they are concerned about the risk of identity information, session cookies and other data being extracted from devices infected with malware, activities highly correlated to a future ransomware attack.[1] https://thehackernews.com/2024/11/5-bcdr-oversights-that-leave-you-exposed-to-ransomware.html

TECHNICAL SUMMARY

EMERGING THREATS & EXPLOITS

- ***LightSpy Spyware Operation Expands to Windows*** - Focused on stealing information from the infected devices, LightSpy was initially detailed in 2020, when it was used in attacks against iPhone users in Hong Kong. https://www.securityweek.com/lightspy-ios-spyware-operation-expands-to-windows/
- ***High-Severity Flaw in PostgreSQL Allows Hackers to Exploit Environment Variables*** - Cybersecurity researchers have disclosed a high-severity security flaw in the PostgreSQL open-source database system that could allow unprivileged users to alter environment variables, and potentially lead to code execution or information disclosure. https://thehackernews.com/2024/11/high-severity-flaw-in-postgresql-allows.html
- ***Palo Alto Networks Patches Critical Zero-Day Firewall Bug -*** Palo Alto Networks (PAN) put out an advisory on Friday, Nov. 15, warning its customers that a critical, unauthenticated remote code execution (RCE) bug is under exploit by cybercriminals in its Expedition firewall interface — making this the tool's fourth vulnerability under active attack identified in just the past week. https://www.darkreading.com/cyberattacks-data-breaches/palo-alto-networks-patches-critical-zero-day-bug-firewalls
- ***Fraud Network Uses 4,700 Fake Shopping Sites To Steal Credit Cards –*** A financially motivated Chinese threat actor dubbed "SilkSpecter" is using thousands of fake online stores to steal the payment card details of online shoppers in the U.S. and Europe. https://www.bleepingcomputer.com/news/security/fraud-network-uses-4-700-fake-shopping-sites-to-steal-credit-cards/
- ***Critical Really Simple Security plugin flaw impacts 4M+ WordPress sites -*** A Really Simple Security plugin flaw affects 4M+ sites, allowing attackers full admin access. It's one of the most critical WordPress vulnerabilities ever. https://securityaffairs.com/171100/hacking/really-simple-security-plugin-flaw-affects-4m-sites.html

ATTACKS, BREACHES & LEAKS

- ***Meow Group Ransomware Hits Equator Worldwide: Data Breach Alert -*** Equator Worldwide, a UK-based logistics and courier service provider, has recently been targeted by the Meow ransomware group. This attack has resulted in the unauthorized access and potential exposure of over 9 GB of sensitive data, including employee personal details, client service agreements, and financial documents**.**. https://www.halcyon.ai/attacks/meow-group-ransomware-hits-equator-worldwide-data-breach-alert
- ***P.I. Burners Inc.Power & Industrial Services Data Breach*** - Power & Industrial Services Corporation provides innovative custom engineered solutions for power generation and industrial markets, specializing in burner parts and assemblies for power boilers. https://www.breachsense.com/breaches/p-i-burners-inc-power-industrial-services-data-breach/
- ***Ransomware Group Play Hits: dairyfarmersofcanada.ca*** - James H. Maloy, Inc. is a construction company providing general contracting, construction management, and design-build services. https://www.breachsense.com/breaches/james-h-maloy-data-breach/
- ***[FOG] – Ransomware Victim: Fifteenfortyseven Critical Systems Realty (1547realty[.]com)*** - The ransomware leak page associated with the victim, identified as Fifteenfortyseven Critical Systems Realty, indicates a significant data compromise. According to the information extracted, a total of 6 GB of sensitive data has been leaked. This data includes various types of sensitive files, which are critical to the company's operations in the data center industry. https://www.hookphish.com/blog/ransomware-group-play-hits-dairyfarmersofcanada-ca/

SECURITY VULNERABILITIES, ALERTS, ADVISORIES, & UPDATES

SUSE Security Updates

1. nodejs18 - https://www.suse.com/support/update/announcement/2024/suse-ru-20244041-1
2. govulncheck-vulndb - https://www.suse.com/support/update/announcement/2024/suse-su-20244042-1

Fedora Security Advisories

1. microcode_ctl –
   a. https://lwn.net/Articles/999060
   b. https://lwn.net/Articles/999061
2. Trafficserver –
   a. https://lwn.net/Articles/999063
   b. https://lwn.net/Articles/999064
   c. https://lwn.net/Articles/999062
3. Libsndfile - https://lwn.net/Articles/999059

Mageia Security Advisories

1. mesa, libdrm - http://advisories.mageia.org/MGAA-2024-0232.html
2. kanboard - http://advisories.mageia.org/MGASA-2024-0366.html
3. radare2 - http://advisories.mageia.org/MGASA-2024-0367.html

Debian Security Advisories

1. postgresql-15 - https://lists.debian.org/debian-security-announce/2024/msg00231.html

Ubuntu Security Notices

1. python - https://ubuntu.com/security/notices/USN-7015-6

Zero Day Initiative Advisories & Updates

1. Intel - https://www.zerodayinitiative.com/advisories/ZDI-24-1613/

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