Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

Daily Open-Source Cyber Report

November 20, 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

Infrastructure Resilience Planning Framework (IRPF)

CISA developed the Infrastructure Resilience Planning Framework (IRPF) to provide an approach for localities, regions, and the private sector to work together to plan for the security and resilience of critical infrastructure services in the face of multiple threats and changes. The primary audience for the IRPF is state, local, tribal, and territorial governments and associated regional organizations; however, the IRPF can be flexibly used by any organization seeking to enhance its resilience planning. It provides resources for integrating critical infrastructure into planning as well as a framework for working regionally and across systems and jurisdictions.

https://www.cisa.gov/resources-tools/resources/infrastructure-resilience-planning-framework-irpf

Additional Resource:

'IRPF Launchpoint' Quick-Start Tool: https://www.cisa.gov/resources-tools/resources/irpf-launchpoint

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

AT-A-GLANCE

Executive News

- FBI, CISA, and NSA Reveal Most Exploited Vulnerabilities Of 2023
- Rail And Pipeline Representatives Push To Dial Back TSA's Cyber Mandates
- Thames Water Dismisses Claims on Cyber-Attacks
- Robots and AI Are Rebuilding the Supply Chain From Ground Up
- Adversarial Advantage: Using Nation-State Threat Analysis To Strengthen U.S. Cybersecurity
- Idaho Man Sentenced to 10 Years in Prison for Hacking, Data Theft, Extortion
- Fleets Explained: Autonomous vehicles

Emerging Threats & Vulnerabilities

- Emmenhtal Loader Uses Scripts to Deliver Lumma and Other Malware
- TA455's Iranian Dream Job Campaign Targets Aerospace with Malware
- New Pxa Stealer Targets Government And Education Sectors For Sensitive Information
- Hamas-Affiliated WIRTE Employs SameCoin Wiper in Disruptive Attacks Against Israel
- High-Severity Vulnerabilities Patched in Zoom, Chrome

Attacks, Breaches, & Leaks

- Ford Investigates Alleged Breach Following Customer Data Leak
- Hive Power Engineering Data Breach
- AnnieMac Data Breach Impacts 171,000 People
- [SAFEPAY] – Ransomware Victim: millerservicecompany[.]com
- Fintech Giant Finastra Investigating Data Breach

EXECUTIVE NEWS

FBI, CISA, and NSA Reveal Most Exploited Vulnerabilities Of 2023
Bleeping Computer, 11/12/2024

The FBI, the NSA, and Five Eyes cybersecurity authorities have released a list of the top 15 routinely exploited vulnerabilities throughout last year, most of them first abused as zero-days. A joint advisory published on Tuesday calls for organizations worldwide to immediately patch these security flaws and deploy patch management systems to minimize their networks' exposure to potential attacks. "In 2023, malicious cyber actors exploited more zero-day vulnerabilities to compromise enterprise networks compared to 2022, allowing them to conduct cyber operations against higher-priority targets," the cybersecurity agencies warned. https://www.bleepingcomputer.com/news/security/fbi-cisa-and-nsa-reveal-most-exploited-vulnerabilities-of-2023/

Rail And Pipeline Representatives Push To Dial Back TSA’s Cyber Mandates
Cyber Scoop, 11/19/2024

House Republicans and representatives from the rail and pipeline industries criticized what they say are overly onerous security regulations during a Tuesday hearing that could be a preview of how cyber rules are handled in the Trump administration. The House Homeland Security Subcommittee on Transportation and Maritime Security hearing focused on the business impact of Transportation Security Administration emergency directives issued weeks after a ransomware hack forced Colonial Pipeline to take offline nearly half of the gasoline and jet fuel on the East Coast. Republican lawmakers largely voiced concerns that those directives and the agency’s recently issued notice of proposed rulemaking on the subject were far too burdensome. https://cyberscoop.com/house-homeland-hearing-tsa-cyber-regulation/

Thames Water Dismisses Claims on Cyber-Attacks
Bleeping Computer, 11/12/2024

Thames Water has dismissed claims of its network being hit by cyber-attacks, despite an article claiming its IT is ‘falling apart’. In the Guardian article published yesterday, it was claimed that underinvestment in IT systems that are critical to the security of London and the south-east’s water has left it prey to cyber-attacks from nation states, some of which have been partly successful, temporarily disabling some operations, according to three sources familiar with the company’s operations. While Thames declined to comment on the record about cyber-attacks, a source at the company said it had “not experienced any cyber-attacks, full stop”. According to sources who spoke to the Guardian, the systems are so antiquated they have been easy for cyber-criminals to attack. https://insight.scmagazineuk.com/thames-water-dismisses-claims-on-cyber-attacks

Robots and AI Are Rebuilding the Supply Chain From Ground Up
PYMNTS, 11/14/2024

Distribution yards, the critical junctions between warehouse facilities and over-the-road (OTR) transportation, have long stood as bottlenecks in supply chain operations. Each day, millions of trailers and containers pass through these yards — where trucks are loaded, unloaded, and dispatched — with inefficiencies that impact the entire logistics network. Historically, this labor-intensive work has relied on human drivers and manual labor, making it susceptible to inefficiencies and human error "Think of anything you're wearing, eating, or building with today. All of that got transferred through these distribution yards, and they've been operated much like they have been for several decades," Andrew Smith, founder and CEO of Outrider, told PYMNTS. https://www.pymnts.com/artificial-intelligence-2/2024/robots-and-ai-are-rebuilding-the-supply-chain-from-ground-up/

Adversarial Advantage: Using Nation-State Threat Analysis To Strengthen U.S. Cybersecurity
Security Intelligence, 11/13/2024

Nation-state adversaries are changing their approach, pivoting from data destruction to prioritizing stealth and espionage. According to the Microsoft 2023 Digital Defense Report, "nation-state attackers are increasing their investments and launching more sophisticated cyberattacks to evade detection and achieve strategic priorities." These actors pose a critical threat to United States infrastructure and protected data, and compromising either resource could put citizens at risk. Thankfully, there's an upside to these malicious efforts: information. By analyzing nation-state tactics, government agencies and private enterprises are better prepared to track, manage and mitigate these attacks. https://securityintelligence.com/articles/adversarial-advantage-using-nation-state-threat-analysis-to-strengthen-us-cybersecurity/

Idaho Man Sentenced to 10 Years in Prison for Hacking, Data Theft, Extortion
Security Week, 11/14/2024

The man, Robert Purbeck, 45, of Meridian, Idaho, attempted to leverage the stolen information to extort and harass one of his victims, a Florida orthodontist. According to court documents, in June 2017, Purbeck purchased from an underground marketplace the credentials for the server of a Griffin, Georgia, medical clinic and then accessed the server to exfiltrate sensitive information. Purbeck stole records containing the names, addresses, dates of birth, and Social Security numbers of more than 43,000 individuals. In February 2018, he purchased credentials for a City of Newnan Police Department server and then accessed it to steal police reports and other documents. Over 14,000 people were affected by the data breach. https://www.securityweek.com/idaho-man-sentenced-to-10-years-in-prison-for-hacking-data-theft-extortion/

Fleets Explained: Autonomous vehicles
Fleet Owner, 11/15/2024

In a world where every digital connection has the potential to be a vulnerability, the stakes for cybersecurity have never been higher. The recent statement from National Security Advisor Jake Sullivan on supply chain security brings into sharp focus the escalating threats faced by critical infrastructure operators, particularly the energy sector. For the United States, securing this sector is not just a matter of national interest; it's a strategic necessity that reverberates across global markets. As the energy sector becomes increasingly intertwined with complex networks of software and IT vendors, the risk of a cyber incident grows exponentially. The integration of industrial control systems (ICS) and energy automation offers operational benefits but also opens doors to significant vulnerabilities.
https://www.fleetowner.com/fleets-explained/article/55243151/fleets-explained-self-driving-trucks-in-the-transportation-industry

TECHNICAL SUMMARY

EMERGING THREATS & EXPLOITS

- ***Emmenhtal Loader Uses Scripts to Deliver Lumma and Other Malware*** - Emmenhtal Loader uses LOLBAS techniques, deploying malware like Lumma and Amadey through legitimate Windows tools. Its infection chain of LNK files and encrypted scripts evades detection. https://hackread.com/emmenhtal-loader-uses-scripts-deliver-lumma-malware/
- ***TA455's Iranian Dream Job Campaign Targets Aerospace with Malware*** - A complex phishing campaign attributed to the Iranian-linked threat actor TA455, has been observed using sophisticated techniques to impersonate job recruiters on LinkedIn and other platforms. https://www.infosecurity-magazine.com/news/ta455s-iranian-dream-job-campaign/
- ***New Pxa Stealer Targets Government And Education Sectors For Sensitive Information* -** The attacker is targeting the education sector in India and government organizations in European countries, including Sweden and Denmark, based on Talos telemetry data. https://blog.talosintelligence.com/new-pxa-stealer/
- ***Hamas-Affiliated WIRTE Employs SameCoin Wiper in Disruptive Attacks Against Israel* –** A threat actor affiliated with Hamas has expanded its malicious cyber operations beyond espionage to carry out disruptive attacks that exclusively target Israeli entities. The activity, linked to a group called WIRTE, has also targeted the Palestinian Authority, Jordan, Iraq, Saudi Arabia, and Egypt, Check Point said in an analysis. https://thehackernews.com/2024/11/hamas-affiliated-wirte-employs-samecoin.html
- ***High-Severity Vulnerabilities Patched in Zoom, Chrome* -** Zoom announced fixes for six security defects, including two high-severity issues that could allow remote attackers to escalate privileges or leak sensitive information. https://www.securityweek.com/high-severity-vulnerabilities-patched-in-zoom-chrome/

ATTACKS, BREACHES & LEAKS

- ***Ford Investigates Alleged Breach Following Customer Data Leak -*** Ford is investigating allegations that it suffered a data breach after a threat actor claimed to leak 44,000 customer records on a hacking forum. The leak was announced on Sunday by threat actor 'EnergyWeaponUser,' also implicating the hacker 'IntelBroker,' who supposedly took part in the November 2024 breach. https://www.bleepingcomputer.com/news/security/ford-investigates-alleged-breach-following-customer-data-leak/
- ***Hive Power Engineering Data Breach*** - Hive Power Engineering LLC (HIVE) provides engineering design and consulting services primarily in the transmission and distribution sector for power utilities. https://www.breachsense.com/breaches/hive-power-engineering-data-breach/
- ***AnnieMac Data Breach Impacts 171,000 People*** - New Jersey-based mortgage loan provider AnnieMac Home Mortgage (American Neighborhood Mortgage Acceptance Company) is informing many individuals of a recent data breach. https://www.securityweek.com/anniemac-data-breach-impacts-171000-people/
- ***[SAFEPAY] – Ransomware Victim: millerservicecompany[.]com*** - The ransomware leak page associated with Oxford Auto Insurance indicates that sensitive data will be fully leaked on November 24, 2024. Currently, there are views logged at 236, suggesting that the page has attracted some attention within the dark web community. However, no download links are provided on the page, which could mean that the data is either not yet available or the threat actors have chosen to restrict access for now. https://www.redpacketsecurity.com/monti-ransomware-victim-oxford-auto-insurance/
- ***Fintech Giant Finastra Investigating Data Breach*** - The financial technology firm Finastra is investigating the alleged large-scale theft of information from its internal file transfer platform, KrebsOnSecurity has learned. Finastra, which provides software and services to 45 of the world's top 50 banks, notified customers of the security incident after a cybercriminal began selling more than 400 gigabytes of data purportedly stolen from the company. https://krebsonsecurity.com/2024/11/fintech-giant-finastra-investigating-data-breach/

SECURITY VULNERABILITIES, ALERTS, ADVISORIES, & UPDATES

US CERT/ ICS CERT Alerts and Advisories

1. BianLian - https://www.cisa.gov/news-events/alerts/2024/11/20/cisa-and-partners-release-update-bianlian-ransomware-cybersecurity-advisory
2. VMware vCenter –
   a. https://www.cve.org/CVERecord?id=CVE-2024-38812
   b. https://www.cve.org/CVERecord?id=CVE-2024-38813

SUSE Security Updates

1. SUSE Manager 5.0: Server, Proxy and Retail Branch Server - https://www.suse.com/support/update/announcement/2024/suse-ru-20244039-1

Mageia Security Advisories

1. 5 thunderbird, thunderbird-l10n - http://advisories.mageia.org/MGASA-2024-0365.html

Debian Security Advisories

1. libmodule-scandeps-perl - https://lists.debian.org/debian-security-announce/2024/msg00230.html
2. needrestart - https://lists.debian.org/debian-security-announce/2024/msg00229.html

Check Point Security Advisories

1. Palo Alto - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-1075.html
2. WordPress - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-1070.html

Red Hat Security Advisories

1. Tigervnc - https://access.redhat.com/errata/RHSA-2024:10090

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

OTHER

1. Safari 18.1.1 - https://support.apple.com/en-us/121756
2. visionOS 2.1.1 - https://support.apple.com/en-us/121755
3. iOS 18.1.1 and iPadOS 18.1.1 - https://support.apple.com/en-us/121752
4. iOS 17.7.2 and iPadOS 17.7.2 - https://support.apple.com/en-us/121754
5. macOS Sequoia 15.1.1 - https://support.apple.com/en-us/121753

***** 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.