Information Sharing &
Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

Daily Open-Source Cyber Report

November 21, 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

Identity Theft

Identity theft happens when someone steals your personal information to commit fraud. The identity thief may use your information to apply for credit, file taxes, or get medical services. These acts can damage your credit status and cost you time and money to restore your good name.

- Don't reveal personally identifiable information such as your bank account number, Social Security Number (SSN), or date of birth to unknown sources.
- Practice safe web surfing wherever you are by checking for the green lock or padlock icon in your browser bar—this signifies a secure connection.
- Type website URLs directly into the address bar instead of clicking on links or copying and pasting from the email.
- Check with the known sender before clicking on any links. All emails and messages should be considered suspicious, when in doubt.

For additional resources to report and recover from identity theft contact the Federal Trade Commission's Identity Theft website: www.identitytheft.gov/#

Additional Resources:

- Preventing and Responding to Identity Theft; Cybersecurity and Infrastructure Security Agency (CISA), 2/1/2022 https://www.cisa.gov/news-events/news/preventing-and-responding-identity-theft
- Identity Theft; U.S. Department of Justice https://www.justice.gov/criminal/criminal-fraud/identity-theft/identity-theft-and-identity-fraud
- Identity Theft Central; U.S. Internal Revenue Service (IRS) https://www.irs.gov/identity-theft-central

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

AT-A-GLANCE

Executive News

- 2024 CWE Top 25 Most Dangerous Software Weaknesses
- Undersea Cables Cut Or Damaged, Leading European Nations To Investigate Possible Sabotage
- U.S. Indicts Snowflake Hackers Who Extorted $2.5 Million From 3 Victims
- Autonomous Trucking: Future Challenges and Opportunities For The Shipping Industry
- Retrofitting Spatial Safety To Hundreds Of Millions Of Lines Of C++
- API Security in Peril as 83% of Firms Suffer Incidents
- Overcoming Cybersecurity Threats

Emerging Threats & Vulnerabilities

- Google AI Platform Bugs Leak Proprietary Enterprise LLMs
- Lazarus Group Targets macOS with RustyAttr Trojan in Fake Job PDFs
- Update Now! Apple Confirms Vulnerabilities Are Already Being Exploited
- New Glove Infostealer Malware Bypasses Chrome’s Cookie Encryption
- Russian Hackers Exploit New NTLM Flaw to Deploy RAT Malware via Phishing Emails

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

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

EXECUTIVE NEWS

2024 CWE Top 25 Most Dangerous Software Weaknesses
CISA, 11/20/2024

The Cybersecurity and Infrastructure Security Agency (CISA), in collaboration with the Homeland Security Systems Engineering and Development Institute (HSSEDI), operated by MITRE, has released the 2024 CWE Top 25 Most Dangerous Software Weaknesses. This annual list identifies the most critical software weaknesses that adversaries frequently exploit to compromise systems, steal sensitive data, or disrupt essential services. Organizations are strongly encouraged to review this list and use it to inform their software security strategies. Prioritizing these weaknesses in development and procurement processes helps prevent vulnerabilities at the core of the software lifecycle. https://www.cisa.gov/news-events/alerts/2024/11/20/2024-cwe-top-25-most-dangerous-software-weaknesses

Undersea Cables Cut Or Damaged, Leading European Nations To Investigate Possible Sabotage
CBS News, 11/20/2024

Two undersea cables carrying internet data deep in the Baltic Sea were damaged, European telecommunications companies said this week, drawing warnings from European governments of possible Russian "hybrid warfare" targeting global communications infrastructure.
On Wednesday, interest was focused on a Chinese-flagged cargo ship called the Yi Peng 3, which data provided by the maritime tracking service Vessel Finder showed to have been in the area around the time the cables were damaged. On Wednesday, interest was focused on a Chinese-flagged cargo ship called the Yi Peng 3, which data provided by the maritime tracking service Vessel Finder showed to have been in the area around the time the cables were damaged.
https://www.cbsnews.com/news/undersea-cables-cut-europe-finland-germany-hint-russia-sabotage/

U.S. Indicts Snowflake Hackers Who Extorted $2.5 Million From 3 Victims
Bleeping Computer, 11/13/2024

The U.S. Department of Justice has unsealed the indictment against two suspected Snowflake hackers, who breached more than 165 organizations using the services of the Snowflake cloud storage company. Connor Riley Moucka and John Erin Binns are accused of using credentials, obtained with the help of info-stealing malware, to hijack Snowflake accounts that were not protected by multi-factor authentication. Moucka and Binns exfiltrated terabytes of data from various companies and demanded ransom payments in exchange for deleting the stolen information. According to the indictment, the two hackers stole "approximately 50 billion customer call and text records" from a "major telecommunications" company in the U.S. https://www.bleepingcomputer.com/news/security/us-indicts-snowflake-hackers-who-extorted-25-million-from-3-victims/

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

Autonomous Trucking: Future Challenges and Opportunities For The Shipping Industry
Dax Street, 11/14/2024

Autonomous vehicles (AVs) have the potential to transform the trucking industry by reducing shipping costs and mitigating the driver shortage. However, according to McKinsey's analysis, their widespread adoption will likely face another year of delay. Despite these challenges, major OEMs are maintaining their commitment to autonomous trucking and investing in the development of these groundbreaking vehicles, aiming for deployment in the latter half of this decade (see sidebar, "The technology underpinning autonomous trucks"). https://daxstreet.com/cars/226167/autonomous-trucking-future-challenges-and-opportunities-for-the-shipping-industry/

Retrofitting Spatial Safety To Hundreds Of Millions Of Lines Of C++
Google Security Blog, 11/15/2024

Attackers regularly exploit spatial memory safety vulnerabilities, which occur when code accesses a memory allocation outside of its intended bounds, to compromise systems and sensitive data. These vulnerabilities represent a major security risk to users. Based on an analysis of in-the-wild exploits tracked by Google's Project Zero, spatial safety vulnerabilities represent 40% of in-the-wild memory safety exploits over the past decade: Google is taking a comprehensive approach to memory safety. A key element of our strategy focuses on Safe Coding and using memory-safe languages in new code. https://security.googleblog.com/2024/11/retrofitting-spatial-safety-to-hundreds.html

API Security in Peril as 83% of Firms Suffer Incidents
Infosecurity Week, 11/14/2024

Security experts have warned of the soaring cost and volume of API security incidents after revealing that 83% of UK organizations were impacted over the past 12 months. Akamai polled 404 UK CIOs, CISOs and other security professionals between June and July 2024, to help compile its API Security Impact Study 2024. It recorded a 14-percentage point annual increase in UK respondents claiming to have experienced at least one API security incident over the previous 12 months. For US respondents, the figure actually dropped two percentage points. In the UK, each incident cost over £420,000 ($532,000) in repairs, downtime, legal fees, fines and other charges – significantly more than the equivalent figure in Germany (£335,277). https://www.infosecurity-magazine.com/news/api-security-83-firms-suffer/

Overcoming Cybersecurity Threats
Machine Design, 11/14/2024

When Colonial Pipeline, the largest refined products pipeline in the United States, experienced a ransomware attack in 2021, the cybercriminals infected the company's digital systems, shutting them down for several days. The hackers also stole sensitive information from the company, forcing Colonial Pipeline to pay $5 million in ransom so the hackers didn't release the data publicly. Not only did this ransomware attack paralyze Colonial Pipeline's operations and cost them millions of dollars, but it also decreased fuel supplies, caused airports to cancel flights and resulted in many Americans panic-buying fuel. The attack was ultimately deemed a national security threat.
https://www.machinedesign.com/automation-iiot/article/55243044/overcoming-cybersecurity-threats

TECHNICAL SUMMARY

EMERGING THREATS & EXPLOITS

- ***Google AI Platform Bugs Leak Proprietary Enterprise LLMs*** - Google has fixed two flaws in Vertex AI, its platform for custom development and deployment of large language models (LLMs), that could have allowed attackers to exfiltrate proprietary enterprise models from the system. The flaw highlights once again the danger that malicious manipulation of artificial intelligence (AI) technology present for business users. https://hackread.com/emmenhtal-loader-uses-scripts-deliver-lumma-malware/
- ***Lazarus Group Targets macOS with RustyAttr Trojan in Fake Job PDFs*** - Group-IB has uncovered Lazarus group's stealthy new trojan and technique of hiding malicious code in extended attributes on macOS. Learn how this advanced persistent threat (APT) is evading detection and the steps you can take to protect yourself. https://hackread.com/lazarus-group-macos-rustyattr-trojan-fake-job-pdfs/
- ***Update Now! Apple Confirms Vulnerabilities Are Already Being Exploited -*** Apple has released security patches for most of its operating systems, including iOS, Mac, iPadOS, Safari, and visionOS. The updates for iOS and Intel-based Mac systems are especially important, as they tackle vulnerabilities that are being actively exploited by cybercriminals. You should make sure you update as soon as you can. https://www.malwarebytes.com/blog/news/2024/11/update-now-apple-confirms-vulnerabilities-are-being-exploited
- ***New Glove Infostealer Malware Bypasses Chrome's Cookie Encryption –*** New Glove Stealer malware can bypass Google Chrome's Application-Bound (App-Bound) encryption to steal browser cookies. As Gen Digital security researchers who first spotted it while investigating a recent phishing campaign said, this information-stealing malware is "relatively simple and contains minimal obfuscation or protection mechanisms," indicating that it's very likely in its early development stages. https://www.bleepingcomputer.com/news/security/new-glove-infostealer-malware-bypasses-google-chromes-cookie-encryption/
- ***Russian Hackers Exploit New NTLM Flaw to Deploy RAT Malware via Phishing Emails -*** A newly patched security flaw impacting Windows NT LAN Manager (NTLM) was exploited as a zero-day by a suspected Russia-linked actor as part of cyber attacks targeting Ukraine. https://thehackernews.com/2024/11/russian-hackers-exploit-new-ntlm-flaw.html

ATTACKS, BREACHES & LEAKS

- ***Interoute Hit by Lynx Ransomware: 50GB Data Compromised -*** Interoute, a Luxembourg-based transportation and logistics company, has recently fallen victim to a ransomware attack orchestrated by the Lynx group. This incident, discovered on November 6, has resulted in the exfiltration of 50 GB of sensitive data, posing significant risks to the company's operations and client confidentiality. https://www.halcyon.ai/attacks/interoute-hit-by-lynx-ransomware-50gb-data-compromised
- ***[QILIN] – Ransomware Victim: Stalcop Metal Forming LLC*** - 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/
- ***James H. Maloy Data Breach*** - 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/
- ***Hackers Redirect $250,000 Payment in iLearningEngines Cyberattack*** - iLearningEngines told the SEC that a threat actor accessed its environment and certain files on its network, deleted some emails, and misdirected a $250,000 wire payment, which has not been recovered. . https://www.securityweek.com/hackers-redirect-250000-payment-in-ilearningengines-cyberattack/
- ***Mexico's President Says Government Is Investigating Reported Ransomware Hack Of Legal Affairs Office*** - Mexico's president said Wednesday that the government is investigating an alleged ransomware hack of her administration's legal affairs office after what appeared to be samples of personal information from a database of government employees were posted online. https://apnews.com/article/mexico-president-hacking-attack-ransomhub-ransomware-a97fa044850ba05f574f71d2af3d67c8

SECURITY VULNERABILITIES, ALERTS, ADVISORIES, & UPDATES

US CERT/ ICS CERT Alerts and Advisories

1. Automated Logic - https://www.cisa.gov/news-events/ics-advisories/icsa-24-326-01
2. OSCAT Basic Library - https://www.cisa.gov/news-events/ics-advisories/icsa-24-326-02
3. Schneider Electric–
   a. https://www.cisa.gov/news-events/ics-advisories/icsa-24-326-03
   b. https://www.cisa.gov/news-events/ics-advisories/icsa-24-326-04
   c. https://www.cisa.gov/news-events/ics-advisories/icsa-24-326-05
   d. https://www.cisa.gov/news-events/ics-advisories/icsa-24-326-06
   e.
4. mySCADA - https://www.cisa.gov/news-events/ics-advisories/icsa-24-326-07

SUSE Security Updates

1. SUSE Manager - https://www.suse.com/support/update/announcement/2024/suse-ru-20244039-1

Drupal Security Advisories

1. Eloqua - https://www.drupal.org/sa-contrib-2024-063
2. Mailjet - https://www.drupal.org/sa-contrib-2024-062
3. Drupal core - https://www.drupal.org/sa-core-2024-008

Red Hat Security Advisories

- RHOSP 17.1.4 –
  - https://access.redhat.com/errata/RHSA-2024:9989
  - https://access.redhat.com/errata/RHSA-2024:9991
  - https://access.redhat.com/errata/RHSA-2024:9976
  - https://access.redhat.com/errata/RHSA-2024:9977

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

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

TOOL NEWS & UPDATES

Tools & Initiatives

- Zeek 6.0.9 - https://packetstormsecurity.com/files/182713/zeek-6.0.9.tar.gz
- Cable .NET Post Exploitation Tool - https://packetstormsecurity.com/files/download/182693/Cable-main.zip
- Wireshark Analyzer 4.4.2 - https://packetstormsecurity.com/files/download/182717/wireshark-4.4.2.tar.xz
- Falco 0.39.2 - https://packetstormsecurity.com/files/182716/falco-0.39.2.tar.gz