Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

# Daily Open-Source Cyber Report

December 27, 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**

- Chinese Cyber Center Points Finger At U.S. Over Alleged Cyberattacks To Steal Trade Secrets
- OT/ICS Engineering Workstations Face Barrage of Fresh Malware
- Ukrainian Raccoon Infostealer Operator Sentenced to Prison in US
- Credential Phishing Attacks Up Over 700 Percent
- Vulnerability Exploit Assessment Tool EPSS Exposed to Adversarial Attack
- Consumers Wrongly Attribute All Data Breaches To Cybercriminals
- Top 5 Freight Fraud Stories Of 2024

**Emerging Threats & Vulnerabilities**

- Earth Koshchei Coopts Red Team Tools in Complex RDP Attacks
- Azure Data Factory Bugs Expose Cloud Infrastructure
- Cybercriminals Exploit Google Calendar to Spread Malicious Links
- Over 25,000 SonicWall VPN Firewalls exposed to critical flaws
- Androxgh0st Botnet Targets IoT Devices, Exploiting 27 Vulnerabilities

**Attacks, Breaches, & Leaks**

- Airline Hit By A Cyberattack, Delaying Flights During The Year-End Holiday Season
- Builder.ai Database Misconfiguration Exposes 1.29 TB of Unsecured Records
- KY: Personal data of Boone, Kenton County students breached, school officials say
- Personal Data Of Millions Exposed After Two Government Sites Hacked
- American Addiction Centers Data Breach Impacts 422,000 People

# Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

## EXECUTIVE NEWS

**Chinese Cyber Center Points Finger At U.S. Over Alleged Cyberattacks To Steal Trade Secrets**
*Cyber Scoop, 12/19/2024*

China's national cyber incident response center accused the U.S. government of launching cyberattacks against two Chinese tech companies in a bid to steal trade secrets. In a notice Wednesday, the National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT) said a suspected U.S. intelligence agency was behind the attacks, and that CNCERT had "handled" them, according to a Google translation. The U.S. government has long accused China of cyber espionage to steal trade secrets from domestic companies, and China's allegations about U.S. cyberattacks arrives in the midst of a very public campaign from U.S. government officials blaming China for a major attack on telecommunications carriers. https://cyberscoop.com/chinese-cyber-center-us-alleged-cyberattacks-trade-secrets/

**OT/ICS Engineering Workstations Face Barrage of Fresh Malware**
*Dark Reading, 12/19/2024*

Operational technology (OT) and Industrial control systems (ICS) are increasingly exposed to compromise through engineering workstations. A new malware developed to kill stations running Siemens systems joins a growing list of botnets and worms working to infiltrate industrial networks through these on-premises, Internet-connected attack vectors. Forescout researchers reported the discovery of the Siemens malware, which they called "Chaya_003." But that's hardly an isolated case. The researchers also found two Mitsubishi engineering workstations compromised by the Ramnit worm, they explained in a new report. "Malware in OT/ICS is more common than you think — and engineering workstations connected to the Internet are targets," the Forescout team warned.
https://www.darkreading.com/vulnerabilities-threats/ot-ics-engineering-workstations-malware

**Ukrainian Raccoon Infostealer Operator Sentenced to Prison in US**
*Infosecurity Magazine, 12/19/2024*

The man, Mark Sokolovsky, 28, was arrested in March 2022 in the Netherlands, after the FBI and law enforcement agencies in Italy and the Netherlands took down the infrastructure behind Raccoon Infostealer. The US announced charges against Sokolovsky in October 2022. In February 2024, he was extradited to the US from the Netherlands, and he pleaded guilty in October 2024 to operating the Raccoon Infostealer malware. According to court documents, Raccoon Infostealer was offered under the malware-as-a-service (MaaS) business model, where miscreants would pay the operator roughly $200 per month in cryptocurrency to lease access to the malware. https://www.securityweek.com/ukrainian-raccoon-infostealer-operator-sentenced-to-prison-in-us/

**Credential Phishing Attacks Up Over 700 Percent**
*Beta News, 12/20/2024*

Phishing remains one of the most significant cyber threats impacting organizations worldwide and a new report shows credential theft attacks surged dramatically in the second half of 2024, rising by 703 percent. The report from SlashNext shows that overall, email-based threats rose by 202 percent over the same period, with individual users receiving at least one advanced phishing link per week capable of bypassing traditional network security controls. SlashNext analyzed billions of threats across email and mobile channels -- including Business Email Compromise (BEC), malicious links, attachments, QR codes, and AI-driven natural language attacks -- the report offers a comprehensive look at the rapidly evolving phishing landscape and the vectors most exploited by cybercriminals in the past year. https://betanews.com/2024/12/18/credential-phishing-attacks-up-over-700-percent/

**Vulnerability Exploit Assessment Tool EPSS Exposed to Adversarial Attack**
*Infosecurity Magazine, 12/19/2024*

In a new proof-of-concept, endpoint security provider Morphisec showed that the Exploit Prediction Scoring System (EPSS), one of the most widely used frameworks for assessing vulnerability exploits, could itself be vulnerable to an AI-powered adversarial attack. Ido Ikar, a Threat Researcher at Morphisec, published his findings in a blog post on December 18. He demonstrated how subtle modifications to vulnerability features can alter the EPSS model's predictions and discussed the implications for cybersecurity. https://www.infosecurity-magazine.com/news/epss-exposed-to-adversarial-attack/

**Consumers Wrongly Attribute All Data Breaches To Cybercriminals**
*EMS Now, 12/15/2024*

Breaches in 2024 had less impact on consumers' trust in brands compared to the previous year (a 6.5% decrease from 62% in 2023 to 58% in 2024), according to a recent Vercara report. Most consumers also remain unaware of the role they may play in cyber incidents. The research reveals that consumers are unaware of the impact of insider threats, and instead assume bad actors are to blame for most attacks. It takes a lot to earn consumer trust, especially after a successful cyberattack. 66% of US consumers would not trust a company that falls victim to a data breach with their data and 44% of consumers attribute cyber incidents to a company's lack of security measures. Interestingly, 54% extend a degree of leniency toward smaller brands grappling with cyberattacks, in contrast to their higher expectations for larger businesses. https://www.helpnetsecurity.com/2024/12/18/data-breach-consumers-trust/

**Top 5 Freight Fraud Stories Of 2024**
*Freight Waves, 12/26/2024*

This year freight fraud took center stage, exposing cracks in the logistics industry's defenses and leaving a trail of financial devastation. From coordinated ransom schemes to pandemic relief fraud, 2024 showcased the growing sophistication and reach of bad actors in transportation. These cases revealed a troubling pattern of exploiting systemic vulnerabilities. Fraudsters used tools like falsified documents, illegal carriers and shell companies to bypass regulations and manipulate financial systems. The industry saw brokers, carriers and investors fall victim to schemes that spanned everything from Ponzi operations to digital freight mismanagement. https://www.freightwaves.com/news/top-5-freight-fraud-stories-of-2024

# Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

## TECHNICAL SUMMARY

### EMERGING THREATS & EXPLOITS

- ***Earth Koshchei Coopts Red Team Tools in Complex RDP Attacks -*** Red teaming provides essential tools and testing methodologies for organizations to strengthen their security defenses. Cybercriminals and advanced persistent threat (APT) actors pay close attention to new methods and tools red teams develop, and they may repurpose them with a malicious intent. https://www.trendmicro.com/en_us/research/24/l/earth-koshchei.html
- ***Azure Data Factory Bugs Expose Cloud Infrastructure*** - Three flaws discovered in the way Microsoft's Azure-based data integration service leverages an open source workflow orchestration platform could have allowed an attacker to achieve administrative control over companies' Azure cloud infrastructures, exposing enterprises to data exfiltration, malware deployment, and unauthorized data access. https://www.darkreading.com/cloud-security/azure-data-factory-bugs-expose-cloud-infrastructure
- ***Cybercriminals Exploit Google Calendar to Spread Malicious Links-*** New research from Check Point has revealed how cybercriminals are bypassing email security measures by using Google Calendar and Drawings to send seemingly legitimate invites containing malicious links. https://www.infosecurity-magazine.com/news/cybercriminals-exploit-google/
- ***Over 25,000 SonicWall VPN Firewalls exposed to critical flaws –*** Over 25,000 publicly accessible SonicWall SSLVPN devices are vulnerable to critical severity flaws, with 20,000 using a SonicOS/OSX firmware version that the vendor no longer supports. https://www.bleepingcomputer.com/news/security/over-25-000-sonicwall-vpn-firewalls-exposed-to-critical-flaws/
- ***Androxgh0st Botnet Targets IoT Devices, Exploiting 27 Vulnerabilities –*** CloudSEK's contextual AI digital risk platform Xvigil has uncovered a significant evolution in the Androxgh0st botnet, revealing its exploitation of over 20 vulnerabilities and operational integration with the Mozi botnet with expected rise of, at least, 75% more web-application vulnerabilities by mid- 2025.This indicates a significant increase in Androxgh0st's initial attack vector arsenal from 11 in November 2024 to around 27 within a month. https://hackread.com/androxgh0st-botnet-iot-devices-exploit-vulnerabilities/

# Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

## ATTACKS, BREACHES & LEAKS

- ***Airline Hit By A Cyberattack, Delaying Flights During The Year-End Holiday Season -*** Japan Airlines said it was hit by a cyberattack Thursday, causing delays to more than 20 domestic flights but the carrier said it was able to stop the onslaught and restore its systems hours later. There was no impact on flight safety, it said. https://apnews.com/article/japan-jal-cyberattack-flights-travel-04fbd4848f3015a77057339a5c90ca32
- ***Builder.ai Database Misconfiguration Exposes 1.29 TB of Unsecured Records*** - Cybersecurity researcher Jeremiah Fowler discovered a 1.2TB database containing over 3 million records of Builder.ai, a London-based AI software and app development company. Discover the risks, lessons learned, and best practices for data security. https://hackread.com/builder-ai-database-misconfiguration-expose-tb-records/
- ***Ky: Personal Data Of Boone, Kenton County Students Breached, School Officials Say -*** Personal data from current and former students in Boone and Kenton County school districts may have been accessed and copied in cyber attacks earlier this month, according to school district announcements. https://databreaches.net/2024/12/24/ky-personal-data-of-boone-kenton-county-students-breached-school-officials-say/
- ***Personal Data Of Millions Exposed After Two Government Sites Hacked*** - The Mi Argentina site and the SUBE card app, two of the government's most important digital platforms, were hacked Wednesday night after suffering a cyber attack. The former is a state-owned app that lets users carry their digital IDs and all relevant legal documentation on their phones, while the latter is the site where they can manage all operations of their public transport payment card. https://buenosairesherald.com/business/tech/personal-data-of-millions-exposed-after-two-government-sites-hacked
- ***American Addiction Centers Data Breach Impacts 422,000 People*** - American Addiction Centers Data Breach Impacts 422,000 People https://www.securityweek.com/american-addiction-centers-data-breach-impacts-422000-people/

# Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

## SECURITY VULNERABILITIES, ALERTS, ADVISORIES, & UPDATES

### SUSE Security Updates

1. google-guest-configs –
    a. https://www.suse.com/support/update/announcement/2024/suse-ru-20244424-1
    b. https://www.suse.com/support/update/announcement/2024/suse-ru-20244426-1
    c. https://www.suse.com/support/update/announcement/2024/suse-ru-20244425-1
2. Pacemaker - https://www.suse.com/support/update/announcement/2024/suse-ru-20244427-1
3. python-grpcio –
    a. https://www.suse.com/support/update/announcement/2024/suse-su-20244429-1
    b. https://www.suse.com/support/update/announcement/2024/suse-su-20244428-1

### Fedora Security Advisories

1. python-sql – https://lwn.net/Articles/1003597
2. Incus - https://lwn.net/Articles/1003593
3. libxml2 - https://lwn.net/Articles/1003594
4. dr_libs - https://lwn.net/Articles/1003592