Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

Daily Open-Source Cyber Report

December 12, 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

- U.S. Sanctions Chinese Firm Over Potentially Deadly Ransomware Attack
- UK Cyber-Attacks Surge as Threats Hit Harder, Warns NCSC
- Dozens Of Popular DDoS Sites Raided Ahead Of Potential Christmas Attacks
- Freight Scams Go Cyber
- Hackers Stole $1.49 Billion in Cryptocurrency to Date in 2024
- Two-Thirds Of Office Workers Bypass Security Protocols
- API Attacks Surge 3000%: Why Cybersecurity Needs to Evolve in 2025

Emerging Threats & Vulnerabilities

- North Korean Kimsuky Hackers Use Russian Email Addresses for Credential Theft Attacks
- IdentityIQ Improper Access Control Vulnerability – CVE-2024-10905
- Mitel Micollab Zero-Day And PoC Exploit Unveiled
- Solana Web3.js Library Backdoored in Supply Chain Attack
- Exploit Released For Critical Whatsup Gold RCE Flaw, Patch Now

Attacks, Breaches, & Leaks

- Ransomware Attack Hits Leading Heart Surgery Device Maker
- Romanian Energy Supplier Electrica Group Is Facing A Ransomware Attack
- Appic Garage Data Breach
- $50 Million Radiant Capital Heist Blamed on North Korean Hackers

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

EXECUTIVE NEWS

U.S. Sanctions Chinese Firm Over Potentially Deadly Ransomware Attack
Reuters, 12/10/2024

The United States sanctioned a Chinese cybersecurity company over an ambitious cyberattack that U.S. Treasury officials say could have killed people. The Treasury said in a statement, opens new tab on Tuesday that the Chengdu-based Sichuan Silence Information Technology Company and one of its employees, Guan Tianfeng, deployed malicious software to more than 80,000 firewalls run by thousands of companies worldwide in April 2020. The malicious software not only stole data, but it was used to deploy ransomware, which paralyzes corporate networks by encrypting data. https://www.nextgov.com/cybersecurity/2024/12/senators-call-investigation-dods-comms-following-chinese-telecom-breach/401431/

UK Cyber-Attacks Surge as Threats Hit Harder, Warns NCSC
Infosecurity Magazine, 12/3/2024

Cyber-attacks are becoming more frequent and severe, posing a greater risk to British organizations and the public, warned the UK's National Cyber Security Centre (NCSC) in its latest Annual Review. The report, published on December 3, shows that the NCSC's Incident Management (IM) team has intervened 430 times out of the 1957 cyber-incident reports it received over the past year, exceeding the 371 needing the agency's involvement in 2023. Of these incidents, 89 were nationally significant, including 12 critical incidents – a threefold increase compared to last year. https://www.infosecurity-magazine.com/news/uk-cyberattacks-surge-ncsc/

Dozens Of Popular DDoS Sites Raided Ahead Of Potential Christmas Attacks
The Record, 12/4/2024

International law enforcement has shut down 27 of the most popular platforms used to carry out distributed denial-of-service (DDoS) attacks, Europol announced in a statement on Wednesday. The operation, conducted across 15 countries — including the U.S., U.K., Australia, Brazil, Canada, and Finland — led to the identification of 300 users of these platforms and the arrest of three administrators in France and Germany. Europol explained that the takedowns were timed ahead of Christmas because the holiday season "has long been a peak period for hackers to carry out some of their most disruptive DDoS attacks, causing severe financial loss, reputational damage, and operational chaos for their victims." https://therecord.media/ddos-sites-takedown-international-law-enforcement-europol

Freight Scams Go Cyber
DC Velocity, 12/3/2024

When it comes to the challenges facing the trucking industry, the standard litany goes something like this: driver turnover, diesel prices … and freight scams. Freight scams have always been there, of course. Thieves will naturally flock to a sector that handles 80,000-pound loads of merchandise conveniently packed into 18-wheelers that are sometimes left alone in a freight yard for the weekend or parked overnight along a lonely stretch of highway. But the problem is getting worse, experts say. That's partly because of the rise of the internet, where thieves can use keystrokes—rather than brute force—to divert freight. It has also opened the door to hackers, who can exploit human error to gain access to sensitive information—information they can then use to cripple a company's networks or hold its databases for ransom. https://www.dcvelocity.com/tech-infrastructure/technology/freight-scams-go-cyber

Hackers Stole $1.49 Billion in Cryptocurrency to Date in 2024
Security Week, 12/3/2024

The total year-to-date losses have dropped compared to last year, when they surpassed $1.75 billion during the period, and were mainly driven by losses of over $359 million in May and of more than $282 million in July. In November, cryptocurrency losses surpassed $71 million, mainly due to hacks ($70,996,200), with only a small percentage lost to rug pulls ($25,300). Total losses were 79% lower compared to November 2023, when they exceeded $343 million. According to Immunefi's crypto losses report (PDF) for November 2024, there were 24 hacking incidents reported last month, and two rug pulls. To date in 2024, there have been 209 specific incidents resulting in cryptocurrency losses.
https://www.securityweek.com/hackers-stole-1-49-billion-in-cryptocurrency-to-date-in-2024/

Two-Thirds Of Office Workers Bypass Security Protocols
Beta News, 11/28/2024

Almost two-thirds of office workers admit they've prioritized productivity over safe cybersecurity practices -- 63 percent also own up to using a corporate device to access social media, messaging or entertainment sites/applications. Research from identity and access management company CyberArk also shows that 80 percent access work applications from personal devices, with C-suite executives being among the worst offenders. This is concerning as 36 percent of employees surveyed disagree that they immediately install security patches or software updates for all their personal devices. At the same time, just over a quarter (26 percent) don't always use a VPN when they access work resources.
https://betanews.com/2024/12/03/two-thirds-of-office-workers-bypass-security-protocols/

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

API Attacks Surge 3000%: Why Cybersecurity Needs to Evolve in 2025
The Cyber Express, 12/9/2024

The rise of Application Programming Interfaces (APIs) has revolutionized how businesses operate, enabling seamless connectivity, data sharing, and enhanced functionalities across platforms. However, as digital ecosystems increasingly pivot towards API-driven operations, cybersecurity experts are observing a surge in API attacks. In fact, new research highlights a staggering 3,000% increase in Distributed Denial of Service (DDoS) attacks targeting APIs, compared to traditional web assets. A recent study detailing over 1.26 billion cyberattacks in Q3 2024 reveals some unsettling trends. Of this massive volume, a significant 271 million were API-focused attacks, reflecting a growing threat that organizations can no longer ignore. https://thecyberexpress.com/api-attacks-surge/

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

TECHNICAL SUMMARY

EMERGING THREATS & EXPLOITS

- ***North Korean Kimsuky Hackers Use Russian Email Addresses for Credential Theft Attacks -*** The North Korea-aligned threat actor known as Kimsuky has been linked to a series of phishing attacks that involve sending email messages that originate from Russian sender addresses to ultimately conduct credential theft. https://thehackernews.com/2024/12/north-korean-kimsuky-hackers-use.html
- ***IdentityIQ Improper Access Control Vulnerability – CVE-2024-10905*** - IdentityIQ 8.4 and all 8.4 patch levels prior to 8.4p2, IdentityIQ 8.3 and all 8.3 patch levels prior to 8.3p5, IdentityIQ 8.2 and all 8.2 patch levels prior to 8.2p8, and all prior versions allow HTTP/HTTPS access to static content in the IdentityIQ application directory that should be protected. https://www.sailpoint.com/security-advisories/identityiq-improper-access-control-vulnerability-cve-2024-10905
- ***Mitel Micollab Zero-Day And PoC Exploit Unveiled –*** A zero-day vulnerability in the Mitel MiCollab enterprise collaboration suite can be exploited to read files containing sensitive data, watchTowr researcher Sonny Macdonald has disclosed, and followed up by releasing a proof-of-concept (PoC) exploit that chains together this zero-day file read vulnerability with CVE-2024-41713, which allows attackers to bypass authentication. https://www.helpnetsecurity.com/2024/12/05/mitel-micollab-zero-day-and-poc-exploit-unveiled/
- ***Solana Web3.js Library Backdoored in Supply Chain Attack –*** Some decentralized application developers this week downloaded backdoored versions of the Solana Web3.js library after an attacker compromised a GitHub account with publish rights. https://www.securityweek.com/solana-web3-js-library-backdoored-in-supply-chain-attack/
- ***Exploit Released For Critical Whatsup Gold RCE Flaw, Patch Now -*** A proof-of-concept (PoC) exploit for a critical-severity remote code execution flaw in Progress WhatsUp Gold has been published, making it critical to install the latest security updates as soon as possible. https://www.bleepingcomputer.com/news/security/exploit-released-for-critical-whatsup-gold-rce-flaw-patch-now/

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

ATTACKS, BREACHES & LEAKS

- ***Ransomware Attack Hits Leading Heart Surgery Device Maker -*** Artivion, a leading manufacturer of heart surgery medical devices, has disclosed a November 21 ransomware attack that disrupted its operations and forced it to take some systems offline. https://www.bleepingcomputer.com/news/security/ransomware-attack-hits-leading-heart-surgery-device-maker/
- ***Romanian Energy Supplier Electrica Group Is Facing A Ransomware Attack*** - Romanian energy supplier Electrica Group is investigating an ongoing ransomware attack impacting its operations. https://securityaffairs.com/171832/hacking/electrica-group-ransomware-attack.html
- ***Appic Garage Data Breach -*** Appic Garage is a software application designed to help garage managers efficiently handle operations such as staff management, inventory control, and other related tasks. https://www.breachsense.com/breaches/appic-garage-data-breach/
- ***$50 Million Radiant Capital Heist Blamed on North Korean Hackers*** - A North Korean threat actor was responsible for the $50 million heist that Radiant Capital fell victim to in October, the decentralized finance (DeFi) project says. https://www.securityweek.com/radiant-capital-50-million-heist-blamed-on-north-korean-hackers/

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

SECURITY VULNERABILITIES, ALERTS, ADVISORIES, & UPDATES

US CERT/ ICS CERT Alerts and Advisories

1. Siemens –
    a. https://www.cisa.gov/news-events/ics-advisories/icsa-24-347-01
    b. https://www.cisa.gov/news-events/ics-advisories/icsa-24-347-02
    c. https://www.cisa.gov/news-events/ics-advisories/icsa-24-347-03
    d. https://www.cisa.gov/news-events/ics-advisories/icsa-24-347-04
    e. https://www.cisa.gov/news-events/ics-advisories/icsa-24-347-05
    f. https://www.cisa.gov/news-events/ics-advisories/icsa-24-347-06
    g. https://www.cisa.gov/news-events/ics-advisories/icsa-24-347-07
    h. https://www.cisa.gov/news-events/ics-advisories/icsa-24-347-08
    i. https://www.cisa.gov/news-events/ics-advisories/icsa-24-347-09
    j. https://www.cisa.gov/news-events/ics-advisories/icsa-24-347-10

SUSE Security Updates

1. govulncheck-vulndb - https://www.suse.com/support/update/announcement/2024/suse-su-20244299-1
2. nodejs20 - https://www.suse.com/support/update/announcement/2024/suse-su-20244300-1
3. socat - https://www.suse.com/support/update/announcement/2024/suse-su-20244302-1
4. buildah - https://www.suse.com/support/update/announcement/2024/suse-su-20244303-1
5. qemu - https://www.suse.com/support/update/announcement/2024/suse-su-20244304-1
6. sles-ltss-release - https://www.suse.com/support/update/announcement/2024/suse-ru-20244305-1
7. java-1_8_0-ibm - https://www.suse.com/support/update/announcement/2024/suse-su-20244306-1

Fedora Security Advisories

1. iaito - https://lwn.net/Articles/1001848
2. radare2 - https://lwn.net/Articles/1001852
3. python3.9 –
    a. https://lwn.net/Articles/1001850
    b. https://lwn.net/Articles/1001851

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

Debian Security Advisories

1. python-aiohttp - https://lists.debian.org/debian-security-announce/2024/msg00244.html

Check Point Security Advisories

1. Cleo - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-1155.html

Red Hat Security Advisories

1. Python –
    a. https://access.redhat.com/errata/RHSA-2024:10979
    b. https://access.redhat.com/errata/RHSA-2024:10978
    c. https://access.redhat.com/errata/RHSA-2024:10980
2. Ruby - https://access.redhat.com/errata/RHSA-2024:10982

Ubuntu Security Notices

1. Linux Kernel –
    a. https://ubuntu.com/security/notices/USN-7156-1
    b. https://ubuntu.com/security/notices/USN-7155-1
    c. https://ubuntu.com/security/notices/USN-7154-1
2. PHP - https://ubuntu.com/security/notices/USN-7153-1
3. AsyncSSH - https://ubuntu.com/security/notices/USN-7108-2

Other

1. Apple –
    a. https://support.apple.com/en-us/121846
    b. https://support.apple.com/en-us/121837
    c. https://support.apple.com/en-us/121838
    d. https://support.apple.com/en-us/121839
    e. https://support.apple.com/en-us/121840
    f. https://support.apple.com/en-us/121842
    g. https://support.apple.com/en-us/121843
    h. https://support.apple.com/en-us/121844
    i. https://support.apple.com/en-us/121845