Information Sharing &
Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

Daily Open-Source Cyber Report

December 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.

AT-A-GLANCE

Executive News

- CISA Issues BOD 25-01, Implementing Secure Practices for Cloud Services
- International Crackdown Disrupts DDoS-For-Hire Operations
- High-Value Shipments At Risk: The Growing Threat Of Strategic Cargo Theft
- Black Basta Ransomware Uses MS Teams, Email Bombing to Spread Malware
- The Future of Communications-Based Train Control
- Researchers Crack Microsoft Azure MFA in an Hour
- Many Companies Have Already Faced An Ai-Based Security Alert

Emerging Threats & Vulnerabilities

- Many Companies Have Already Faced An Ai-Based Security Alert
- Chinese EagleMsgSpy Spyware Found Exploiting Mobile Devices Since 2017
- Secret Blizzard Targets Ukrainian Military with Custom Malware
- Microsoft Ships Urgent Patch for Exploited Windows CLFS Zero-Day
- Wpforms Bug Allows Stripe Refunds On Millions Of Wordpress Sites

Attacks, Breaches, & Leaks

- [AKIRA] – Ransomware Victim: Freightliner of Savannah
- Freight Company Delmar Refused To Pay Ransom When Hackers Breached Ssns And Other Data
- Hacker Leaks Cisco Data
- Granite School District Breach Worse Than The District Has Revealed — Former Employee

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

CISA Issues BOD 25-01, Implementing Secure Practices for Cloud Services
CISA, 12/17/2024

Today, CISA issued Binding Operational Directive (BOD) 25-01, Implementing Secure Practices for Cloud Services to safeguard federal information and information systems. This Directive requires federal civilian agencies to identify specific cloud tenants, implement assessment tools, and align cloud environments to CISA's Secure Cloud Business Applications (SCuBA) secure configuration baselines. Recent cybersecurity incidents highlight the significant risks posed by misconfigurations and weak security controls, which attackers can use to gain unauthorized access, exfiltrate data, or disrupt services. https://www.cisa.gov/news-events/alerts/2024/12/17/cisa-issues-bod-25-01-implementing-secure-practices-cloud-services

International Crackdown Disrupts DDoS-For-Hire Operations
Cyber Scoop, 12/12/2024

In a sweeping international crackdown, law enforcement agencies from 15 countries, including the United States and multiple European nations, have dismantled 27 of the most popular platforms used for carrying out distributed denial-of-service (DDoS) attacks, Europol announced Wednesday. The operation, known as PowerOFF, has led to the arrest of three administrators in France and Germany and identified 300 users of these illegal services. Booter and stresser websites allow individuals to launch overwhelming amounts of traffic at targeted websites, effectively rendering them inaccessible. https://cyberscoop.com/international-crackdown-disrupts-ddos-for-hire-operations/

High-Value Shipments At Risk: The Growing Threat Of Strategic Cargo Theft
WTW, 12/17/2024

A steep rise in the number of 'strategic thefts' worldwide has cargo owners investigating ways to tighten supply-chain operations without interrupting the flow of trade. In North America, overall cargo thefts rose a comparative 49% in the first half this year (2024) as increasingly tech-savvy thieves targeted warehouses and shipments moving by land. According to that account, the average loss per shipment grew 83% for the period (against 1H 2023), highlighting the growing ability of criminals to specifically target shipments of high-value goods. https://www.wtwco.com/en-us/insights/2024/12/high-value-shipments-at-risk-the-growing-threat-of-strategic-cargo-theft

Black Basta Ransomware Uses MS Teams, Email Bombing to Spread Malware
Hack Read, 12/10/2024

Cybersecurity researchers at Rapid7 have released a new report detailing its investigation of a sophisticated social engineering campaign launched by the infamous Black Basta ransomware group (aka UNC4393), threatening organizations worldwide. Researchers have observed a resurgence of activity in relation to Black Basta ransomware operators' currently ongoing social engineering campaign, first reported in May 2024 and updated in August 2024. The attackers have now refined their early stages procedures, including new malware payloads, improved delivery, and increased defence evasion, with lures sent via Microsoft Teams. https://hackread.com/black-basta-gang-ms-teams-email-bombing-malware/

The Future of Communications-Based Train Control
Highways Today, 12/10/2024

As the rail industry embraced Communications-Based Train Control, its core goals were explicit: boosting capacity while elevating safety. Today, under the banner of 'smart railways,' these ambitions have expanded, fuelled by a blend of technologies thriving on the robust CBTC foundation. Some hail CBTC as the 'gold standard' of modern rail signalling; others adopt a more measured view. What's indisputable is its revolutionary impact, reshaping the rail signalling concept for decades or even centuries to come. Though CBTC evolution is ongoing, it has already shattered barriers to innovation, enabling bolder strategic visions and achievements in the rail industry. https://highways.today/2024/12/19/communications-train-control/

Researchers Crack Microsoft Azure MFA in an Hour
Dark Reading, 12/11/2024

Researchers cracked a Microsoft Azure method for multifactor authentication (MFA) in about an hour, due to a critical vulnerability that allowed them unauthorized access to a user's account, including Outlook emails, OneDrive files, Teams chats, Azure Cloud, and more. Researchers at Oasis Security discovered the flaw, which was present due to a lack of rate limit for the amount of times someone could attempt to sign in with MFA and fail when trying to access an account, they revealed in a blog post on Dec. 11. The flaw exposed the more than 400 million paid Microsoft 365 seats to potential account takeover, they said. https://www.darkreading.com/cyberattacks-data-breaches/researchers-crack-microsoft-azure-mfa-hour

Many Companies Have Already Faced An Ai-Based Security Alert
Tech Radar, 12/11/2024

A growing number of companies are now facing AI-accentuated security threats as the technology becomes more widespread, new research has claimed. A report from Kong found one-quarter of firms claiming they have encountered AI-enhanced security threats, but as many as three-quarters say they're seriously concerned about them in the future. Furthermore, more than half (55%) have experienced an API security incident in the past year despite the majority (85%) stating that they're confident in their organization's security capabilities. https://www.techradar.com/pro/security/many-companies-have-already-faced-an-ai-based-security-alert

TECHNICAL SUMMARY

EMERGING THREATS & EXPLOITS

- ***New DCOM Attack Exploits Windows Installer for Backdoor Access -*** Cybersecurity researchers at Deep Instinct have uncovered a novel and powerful Distributed Component Object Model (DCOM) based lateral movement attack method that enables attackers to stealthily deploy backdoors on target Windows systems. https://hackread.com/dcom-attack-exploits-windows-installer-backdoor-access/
- ***Chinese EagleMsgSpy Spyware Found Exploiting Mobile Devices Since 2017*** - Cybersecurity researchers have discovered a novel surveillance program that's suspected to be used by Chinese police departments as a lawful intercept tool to gather a wide range of information from mobile devices. https://thehackernews.com/2024/12/chinese-eaglemsgspy-spyware-found.html
- ***Secret Blizzard Targets Ukrainian Military with Custom Malware -*** Russian state threat actor Secret Blizzard has leveraged resources and tools used by other cyber groups to support the Kremlin's military efforts in Ukraine, according to Microsoft. https://www.infosecurity-magazine.com/news/secret-blizzard-ukrainian-military/
- ***Microsoft Ships Urgent Patch for Exploited Windows CLFS Zero-Day –*** Software giant Microsoft on Tuesday rolled out patches for more than 70 documented security defects and called urgent attention to an already-exploited zero-day in the Windows Common Log File System (CLFS). https://www.securityweek.com/microsoft-ships-urgent-patch-for-exploited-windows-clfs-zero-day/
- ***Wpforms Bug Allows Stripe Refunds On Millions Of Wordpress Sites –*** A vulnerability in WPForms, a WordPress plugin used in over 6 million websites, could allow subscriber-level users to issue arbitrary Stripe refunds or cancel subscriptions. https://www.bleepingcomputer.com/news/security/wpforms-bug-allows-stripe-refunds-on-millions-of-wordpress-sites/

ATTACKS, BREACHES & LEAKS

- ***[AKIRA] – Ransomware Victim: Freightliner of Savannah -*** The leak associated with Freightliner Of Savannah, a transportation and logistics company based in Georgia, highlights a significant compromise of sensitive corporate information. https://www.redpacketsecurity.com/akira-ransomware-victim-freightlinerof-savannah/
- ***Freight Company Delmar Refused To Pay Ransom When Hackers Breached Ssns And Other Data*** - The US arm of Canadian freight company Delmar International this week confirmed it notified and undisclosed number of people about a November 2024 data breach that compromised the following personal info: https://www.comparitech.com/news/freight-company-delmar-refused-to-pay-ransom-when-hackers-breached-ssns-and-other-data/
- ***Hacker Leaks Cisco Data -*** A hacker has leaked data stolen recently from a Cisco DevHub instance, but claims it's only a fraction of the total amount of files that was taken. https://www.securityweek.com/hacker-leaks-cisco-data/
- ***Granite School District Breach Worse Than The District Has Revealed — Former Employee*** - Some former employees of Granite School District in Utah are reporting frustration and anger with the district's incident response to an attack by the Rhysida group. One has written up what he found when he examined the publicly leaked data. https://databreaches.net/2024/12/17/granite-school-district-breach-worse-than-the-district-has-revealed-former-employee/

SECURITY VULNERABILITIES, ALERTS, ADVISORIES, & UPDATES

US CERT/ ICS CERT Alerts and Advisories

1. Fortinet - https://www.cisa.gov/news-events/alerts/2024/12/20/fortinet-releases-security-updates-fortimanager

SUSE Security Updates

1. Sudo - https://www.suse.com/support/update/announcement/2024/suse-su-20244389-1
2. Haproxy - https://www.suse.com/support/update/announcement/2024/suse-su-20244390-1
3. docker-stable - https://www.suse.com/support/update/announcement/2024/suse-ru-20244391-1
4. emacs - https://www.suse.com/support/update/announcement/2024/suse-su-20244392-1
5. python-grpcio - https://www.suse.com/support/update/announcement/2024/suse-su-20244393-1
6. python-aiohttp - https://www.suse.com/support/update/announcement/2024/suse-su-20244396-1
7. pacemaker - https://www.suse.com/support/update/announcement/2024/suse-ru-20244399-1
8. grpc - https://www.suse.com/support/update/announcement/2024/suse-su-20244400-1
9. libzypp –
    a. https://www.suse.com/support/update/announcement/2024/suse-ru-20244406-1
    b. https://www.suse.com/support/update/announcement/2024/suse-ru-20244405-1
    c. https://www.suse.com/support/update/announcement/2024/suse-ru-20244403-1

Fedora Security Advisories

1. Jupyterlab –
    a. https://lwn.net/Articles/1002983
    b. https://lwn.net/Articles/1002984

Debian Security Advisories

1. Chromium - https://lists.debian.org/debian-security-announce/2024/msg00250.html

Check Point Security Advisories

1. GeoServer - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-0559.html

Ubuntu Security Notices

1. Linux Kernel –
    a. https://ubuntu.com/security/notices/USN-7166-3
    b. https://ubuntu.com/security/notices/USN-7159-4

Zero Day Initiative Advisories & Updates

1. Delta Electronics –
    a. https://www.zerodayinitiative.com/advisories/ZDI-24-1721/
    b. https://www.zerodayinitiative.com/advisories/ZDI-24-1722/
    c. https://www.zerodayinitiative.com/advisories/ZDI-24-1723/
    d. https://www.zerodayinitiative.com/advisories/ZDI-24-1724/
2. Webadmin - https://www.zerodayinitiative.com/advisories/ZDI-24-1725/
3. Linux Kernel - https://www.zerodayinitiative.com/advisories/ZDI-24-1726/

Oracle Linux Security Update

1. unbound:1.16.2 - https://lwn.net/Articles/1003003
2. python3.11-urllib3 - https://lwn.net/Articles/1002999
3. pam - https://lwn.net/Articles/1002998
4. libsndfile:1.0.31 - https://lwn.net/Articles/1002995
5. mpg123:1.32.9 - https://lwn.net/Articles/1002997
6. skopeo - https://lwn.net/Articles/1003001
7. edk2:20240524 - https://lwn.net/Articles/1002988
8. containernetworking-plugins - https://lwn.net/Articles/1002986