Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

Daily Open-Source Cyber Report

December 3, 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

- Google Deindexes Chinese Propaganda Network
- Sensitive Dot Documents Found Vulnerable To Hackers
- DOJ: Man Hacked Networks To Pitch Cybersecurity Services
- Game of Emperor: Unveiling Long Term Earth Estries Cyber Intrusions
- Telematics and Tracking Systems to Prevent Car Theft
- Blue Yonder Cyberattack: How Prepared Are You If Your TMS or WMS Goes Down?
- Advanced Threat Predictions For 2025

Emerging Threats & Vulnerabilities

- Malware Exploits Trusted Avast Anti-Rootkit Driver to Disable Security Software
- QNAP Addresses Critical Flaws Across NAS, Router Software
- Finding Vulnerabilities In Clipsp, The Driver At The Core Of Windows' Client License Platform
- Russia-Linked Apt Tag-110 Uses Targets Europe And Asia
- Cybersecurity Blind Spots in IaC and PaC Tools Expose Cloud Platforms to New Attacks

Attacks, Breaches, & Leaks

- Medusa Ransomware Hits Logistical Software Ltd in UK Attack
- T-Mobile Claims Salt Typhoon Did Not Access Customer Data
- Hackers Stole Millions Of Dollars From Uganda Central Bank
- Bologna FC Confirms Data Breach After Ransomhub Ransomware Attack

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

EXECUTIVE NEWS

Google Deindexes Chinese Propaganda Network
Cyber Scoop, 11/25/2024

A network of four public relations (PR) firms has been operating pro-China influence operations online since at least 2022, according to Google. In a report published on November 22, Google's Threat Intelligence Group revealed it has removed hundreds of domains from its search and news indexes. These domains were part of a complex ecosystem of four companies running two newswire services pushing pro-Chinese propaganda to international audiences – a network tracked by Google as GlassBridge. Each firm poses as an independent outlet that republishes articles from Chinese state media, press releases, and other content likely commissioned by other PR agency clients.
https://www.infosecurity-magazine.com/news/google-deindexes-chinese/

Sensitive Dot Documents Found Vulnerable To Hackers
Freight Waves, 11/27/2024

Vulnerability tests conducted at the U.S. Department of Transportation revealed that employees' personal information and other sensitive documents are at risk because of ineffective IT safeguards, according to a federal watchdog. By using publicly available administrator account credentials, auditors at the department's Office of Inspector General were able to gain unauthorized access to printers used by employees at DOT's Federal Highway Administration, according to OIG's report published on Wednesday. That access allowed investigators to see all kinds of personal information that employees had previously printed, scanned or faxed, including marriage licenses, medical billings and prescriptions, employee last wills and testaments, tax documents, bank account statements, home addresses, and Social Security numbers. https://www.freightwaves.com/news/sensitive-dot-documents-found-vulnerable-to-hackers

DOJ: Man Hacked Networks To Pitch Cybersecurity Services
Bleeping Computer, 11/25/2024

A Kansas City man has been indicted for allegedly hacking into computer networks and using this access to promote his cybersecurity services. According to the Department of Justice, Nicholas Michael Kloster, 31, of Kansas City, Missouri, breached two computer networks, a health club business and a nonprofit organization. According to the indictment unsealed on Friday, Kloster had been involved in at least three incidents investigated by the FBI against an equal number of organizations not named in the document. The first incident occurred on April 26, 2024, around midnight, when Kloster breached the premises of a health club that operates multiple gyms in the state and gained access to its systems.
https://www.bleepingcomputer.com/news/security/doj-man-hacked-networks-to-pitch-cybersecurity-services/

Game of Emperor: Unveiling Long Term Earth Estries Cyber Intrusions
Trend Micro, 11/25/2024

Since 2023, Earth Estries (aka Salt Typhoon, FamousSparrow, GhostEmperor and UNC2286) has emerged as one of the most aggressive Chinese advanced persistent threat (APT) groups, primarily targeting critical industries such as telecommunications and government entities in the US, the Asia-Pacific region, the Middle East, and South Africa. In this blog entry, we will highlight their evolving attack techniques and analyze the motivation behind their operations, providing insights into their long-term targeted attacks. A key finding from our recent investigation is the discovery of a new backdoor, GHOSTSPIDER, identified during attacks on Southeast Asian telecommunications companies. We will explore the technical details of GHOSTSPIDER, its impact across multiple countries, and interesting findings when we were tracking its command-and-control (C&C) infrastructure.
https://www.trendmicro.com/en_us/research/24/k/earth-estries.html

Telematics and Tracking Systems to Prevent Car Theft
Global Fleet, 11/26/2024

The vehicles most targeted by thieves were those commonly used by car fleets, including Nissan Versa, Kenworth, and Nissan NP300, according to data recorded between October 2023 to September 2024 from the Mexican Association of Insurance Institutions (AMIS). Out of all the insurance vehicles stolen, only 41.4%, equivalent to 25,553 units, were successfully recovered during the period, according to AMIS. With these statistics, many fleet managers and users are seeking solutions to enhance their vehicle security. Telematics and GPS tracking technologies have emerged as the answers to prevent car thefts. https://www.globalfleet.com/en/fleet-strategy/latin-america/features/telematics-and-tracking-systems-prevent-car-theft?t%5B0%5D=Safety&t%5B1%5D=Mexico&t%5B2%5D=Telematics&curl=1

Blue Yonder Cyberattack: How Prepared Are You If Your TMS or WMS Goes Down?
Talking Logistics, 11/25/2024

When a cyberattack takes down your TMS, WMS, or other supply chain software (it's a question of when, not if), will you be ready to respond as effectively as possible or will everyone on your team look at each other and frantically ask, "What do we do now?" I wrote that back in June 2024 in a post titled, "When A Cyberattack Takes Down Your Supply Chain Software." This week, Starbucks, Sainsbury's, Morrisons, and other companies are learning how prepared they are to deal with a cyberattack on one of their supply chain software vendors — specifically, Blue Yonder, which is dealing with a ransomware attack at the moment. As reported by CNN, the attack is "affecting a private cloud computing service the company provides some customers, but not the company's public cloud environment."
https://talkinglogistics.com/2024/11/26/blue-yonder-cyberattack-how-prepared-are-you-if-your-tms-or-wms-goes-down/

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

Advanced Threat Predictions For 2025
Secure List, 11/25/2024

We at Kaspersky's Global Research and Analysis Team monitor over 900 APT (advanced persistent threat) groups and operations. At the end of each year, we take a step back to assess the most complex and sophisticated attacks that have shaped the threat landscape. These insights enable us to anticipate emerging trends and build a clearer picture of what the APT landscape may look like in the year ahead. In this article in the KSB series, we review the trends of the past year, reflect on the predictions we made for 2024, and offer insights into what we can expect in 2025. https://securelist.com/ksb-apt-predictions-2025/114582/

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

TECHNICAL SUMMARY

EMERGING THREATS & EXPLOITS

- ***Malware Exploits Trusted Avast Anti-Rootkit Driver to Disable Security Software -*** Malware exploits legitimate Avast anti-rootkit driver to disable security software. Trellix researchers uncover the attack and provide mitigation steps. https://hackread.com/malware-avast-anti-rootkit-driver-bypass-security/
- ***QNAP Addresses Critical Flaws Across NAS, Router Software*** - QNAP has released security bulletins over the weekend, which address multiple vulnerabilities, including three critical severity flaws that users should address as soon as possible. https://www.bleepingcomputer.com/news/security/qnap-addresses-critical-flaws-across-nas-router-software/
- ***Finding Vulnerabilities In Clipsp, The Driver At The Core Of Windows' Client License Platform –*** ClipSP (clipsp.sys) is a Windows driver used to implement client licensing and system policies on Windows 10 and 11 systems. Cisco Talos researchers have discovered eight vulnerabilities related to clipsp.sys ranging from signature bypass to elevation of privileges and sandbox escape https://blog.talosintelligence.com/finding-vulnerabilities-in-clipsp-the-driver-at-the-core-of-windows-client-license-platform/
- ***Russia-Linked Apt Tag-110 Uses Targets Europe And Asia –*** Insikt Group researchers uncovered an ongoing cyber-espionage campaign by Russia-linked threat actor TAG-110 that employed custom malware tools HATVIBE and CHERRYSPY. The campaign primarily targeted government entities, human rights groups, and educational institutions in Central Asia, East Asia, and Europe. https://securityaffairs.com/171343/apt/tag-110-targets-asia-europe.html
- ***Cybersecurity Blind Spots in IaC and PaC Tools Expose Cloud Platforms to New Attacks -*** Cybersecurity researchers have disclosed two new attack techniques against infrastructure-as-code (IaC) and policy-as-code (PaC) tools like HashiCorp's Terraform and Styra's Open Policy Agent (OPA) that leverage dedicated, domain-specific languages (DSLs) to breach cloud platforms and exfiltrate data. https://thehackernews.com/2024/11/cybersecurity-flaws-in-iac-and-pac.html

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

ATTACKS, BREACHES & LEAKS

- ***Medusa Ransomware Hits Logistical Software Ltd in UK Attack -*** On November 15, Logistical Software Ltd., a UK-based company specializing in logistics software solutions, became the latest victim of a ransomware attack by the notorious Medusa group. This attack highlights the vulnerabilities faced by companies in the logistics sector, particularly those providing critical software services. https://www.halcyon.ai/attacks/medusa-ransomware-hits-logistical-software-ltd-in-uk-attack
- ***T-Mobile Claims Salt Typhoon Did Not Access Customer Data*** - A notorious Chinese hacking group that breached several US telecoms providers was repelled by T-Mobile's cyber-defenses before being able to access any sensitive customer information, the firm's CSO, Jeff Simon, has claimed. https://www.infosecurity-magazine.com/news/tmobile-salt-typhoon-did-not/
- ***Hackers Stole Millions Of Dollars From Uganda Central Bank -*** Ugandan officials confirmed on Thursday that the national central bank suffered a security breach by financially-motivated threat actors. The police's Criminal Investigations Department and the Auditor General are investigating the incident. https://securityaffairs.com/171562/security/financially-motivated-threat-actors-hacked-ugandas-central-bank.html
- ***Bologna FC Confirms Data Breach After Ransomhub Ransomware Attack*** - Bologna Football Club 1909 has confirmed it suffered a ransomware attack after its stolen data was leaked online by the RansomHub extortion group. The Italian football team warns not to download or disseminate any of the stolen data, claiming it is a "serious criminal offense." https://www.bleepingcomputer.com/news/security/bologna-fc-confirms-data-breach-after-ransomhub-ransomware-attack/

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. Ruijie - https://www.cisa.gov/news-events/ics-advisories/icsa-24-338-01
2. Siemens - https://www.cisa.gov/news-events/ics-advisories/icsa-24-338-02
3. Open Automation Software - https://www.cisa.gov/news-events/ics-advisories/icsa-24-338-03
4. ICONICS and Mitsubishi Electric –
    a. https://www.cisa.gov/news-events/ics-advisories/icsa-24-338-04
    b. https://www.cisa.gov/news-events/ics-advisories/icsa-24-184-03
5. Fuji Electric –
    a. https://www.cisa.gov/news-events/ics-advisories/icsa-24-338-05
    b. https://www.cisa.gov/news-events/ics-advisories/icsa-24-338-06
6. ETIC Telecom - https://www.cisa.gov/news-events/ics-advisories/icsa-22-307-01

SUSE Security Updates

1. google-cloud-sap-agent - https://www.suse.com/support/update/announcement/2024/suse-ru-20244144-1
2. wget - https://www.suse.com/support/update/announcement/2024/suse-su-20244145-1
3. php7 - https://www.suse.com/support/update/announcement/2024/suse-su-20244146-1
4. MozillaThunderbird - https://www.suse.com/support/update/announcement/2024/suse-su-20244148-1
5. Libica - https://www.suse.com/support/update/announcement/2024/suse-ru-20244149-1
6. go1.22-openssl - https://www.suse.com/support/update/announcement/2024/suse-ru-20244150-1
7. python - https://www.suse.com/support/update/announcement/2024/suse-su-20244151-1
8. editorconfig-core-c - https://www.suse.com/support/update/announcement/2024/suse-su-20244152-1
9. python310 - https://www.suse.com/support/update/announcement/2024/suse-su-20244153-1
10. sles15-image - https://www.suse.com/support/update/announcement/2024/suse-ru-20244156-1
11. bpftool - https://www.suse.com/support/update/announcement/2024/suse-su-20244157-1

Mageia Security Advisories

1. glib2.0 - http://advisories.mageia.org/MGASA-2024-0386.html
2. haproxy - http://advisories.mageia.org/MGAA-2024-0234.html
3. krb5 - http://advisories.mageia.org/MGASA-2024-0385.html

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

Red Hat Security Advisories

1. firefox - https://access.redhat.com/errata/RHSA-2024:10742
2. thunderbird - https://access.redhat.com/errata/RHSA-2024:10748
3. postgresql:12 - https://access.redhat.com/errata/RHSA-2024:10750
4. rhc - https://access.redhat.com/errata/RHSA-2024:10759

Ubuntu Security Notices

1. HAProxy –
    a. https://ubuntu.com/security/notices/USN-7133-1
    b. https://ubuntu.com/security/notices/USN-7135-1
2. Firefox - https://ubuntu.com/security/notices/USN-7134-1

Zero Day Initiative Advisories & Updates

1. XnSoft XnView - https://www.zerodayinitiative.com/advisories/ZDI-24-1640/
2. Hewlett –
    a. https://www.zerodayinitiative.com/advisories/ZDI-24-1639/
    b. https://www.zerodayinitiative.com/advisories/ZDI-24-1638/
    c. https://www.zerodayinitiative.com/advisories/ZDI-24-1637/

Other

1. Google –
    a. https://chromereleases.googleblog.com/2024/12/stable-channel-update-for-desktop.html
    b. https://chromereleases.googleblog.com/2024/12/extended-stable-updates-for-desktop.html