Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

Daily Open-Source Cyber Report

November 1, 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

Critical Infrastructure Security and Resilience (CISR) Month 2024: Resolve to be Resilient!

Each year, the Cybersecurity and Infrastructure Security Agency (CISA) leads the national recognition of Critical Infrastructure Security and Resilience (CISR) Month in November… As a nation, we are grappling with continued cyber and physical threats to critical infrastructure Americans rely on every day. We have seen increasing threats of violence targeted at faith-based organizations, election workers, and others; extended, record-breaking heat and destructive weather and fire events; global conflicts with ripple effects around the world, including civil disturbances at home; and rapid advances in technology that enable novel cybersecurity risks. The safety and security of the nation depends on the ability of critical infrastructure owners and operators to prepare for and adapt to changing conditions and to withstand and recover rapidly from disruptions. We must accept that it's a whole of community responsibility to prepare and secure the nation's critical infrastructure and protect the vital services it provides, so when something does happen, we are better able to respond to and recover from any impacts. We can do this by building resilience into our preparedness planning year around by understanding the threat landscape and assessing risks; creating and exercising actionable plans; and continually adapting and improving based on lessons learned.

https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-security-and-resilience-month

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

AT-A-GLANCE

Executive News

- Foreign Threat Actor Conducting Large-Scale Spear-Phishing Campaign with RDP Attachments
- U.S., Israel Describe Iranian Hackers' Targeting of Olympics, Surveillance Cameras
- Report Shows AI Fraud, Deepfakes Are Top Challenges For Banks
- Ransomware Remains Top Cybersecurity Concern For Trucking Industry
- AI Chatbots Ditch Guardrails After 'Deceptive Delight' Cocktail
- Talos Ir Trends Q3 2024: Identity-Based Operations Loom Large
- Third-Party Identities: The Weakest Link in Your Cybersecurity Supply Chain

Emerging Threats & Vulnerabilities

- DLL hijacking in TOTOLINK A600UB Driver Installer
- New Attack Lets Hackers Downgrade Windows to Exploit Patched Flaws
- CloudScout: Evasive Panda Scouting Cloud Services
- Android Malware FakeCall Intercepts Your Calls To The Bank
- Lazarus Group Exploits Google Chrome Vulnerability to Control Infected Devices

Attacks, Breaches, & Leaks

- France's Second-Largest Telecoms Provider Free Suffered A Cyber Attack
- Texas County Says 47,000 Had Ssns, Medical Treatment Info Leaked During May Cyberattack
- Henry Schein Discloses Data Breach A Year After Ransomware Attack
- Cardiology Of Virginia Patient Data Appears To Be Up For Sale. Has The Entity Issued Any Statement At All?

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

EXECUTIVE NEWS

Foreign Threat Actor Conducting Large-Scale Spear-Phishing Campaign with RDP Attachments
CISA, 10/31/2024

CISA has received multiple reports of a large-scale spear-phishing campaign targeting organizations in several sectors, including government and information technology (IT). The foreign threat actor, often posing as a trusted entity, is sending spear-phishing emails containing malicious remote desktop protocol (RDP) files to targeted organizations to connect to and access files stored on the target's network. Once access has been gained, the threat actor may pursue additional activity, such as deploying malicious code to achieve persistent access to the target's network. CISA, government, and industry partners are coordinating, responding, and assessing the impact of this campaign. CISA urges organizations to take proactive measures: https://www.cisa.gov/news-events/alerts/2024/10/31/foreign-threat-actor-conducting-large-scale-spear-phishing-campaign-rdp-attachments

U.S., Israel Describe Iranian Hackers' Targeting of Olympics, Surveillance Cameras
Security Week, 11/1/2024

The FBI has been tracking this group's activities since 2020. The threat actor is known in the private sector as Cotton Sandstorm, Marnanbridge, and Haywire Kitten, but it's probably best known as Emennet Pasargad, the name of the company that was until recently used as a front for the group's activities. According to the new advisory written by the FBI, the US Department of Treasury and Israel's National Cyber Directorate, since mid-2024 the name of the front company has been Aria Sepehr Ayandehsazan (ASA). The company, which has been legally registered in Iran, is used for finance-related and HR purposes, among others. Emennet Pasargad and now Aria Sepehr Ayandehsazan officially have been providing cybersecurity services within Iran, including to government organizations. https://www.securityweek.com/us-israel-describe-iranian-hackers-targeting-of-olympics-surveillance-cameras/

Report: Chinese Hackers Used Telecom Access To Go After Phones Of Trump, Vance
Cyber Scoop, 10/25/2024

Federal authorities say they are investigating "unauthorized access to telecommunications commercial infrastructure" from Chinese hackers as news reports allege that the hackers may have used that access to target the phones and data of Republican presidential candidate Donald Trump and vice-presidential candidate J.D. Vance. In a joint statement released Friday, the FBI and the Cybersecurity and Infrastructure Security Agency said they are investigating a breach into U.S. telecommunications infrastructure "by actors affiliated with the People's Republic of China." "After the FBI identified specific malicious activity targeting the sector, the FBI and [CISA] immediately notified affected companies, rendered technical assistance, and rapidly shared information to assist other potential victims, agencies wrote. https://cyberscoop.com/report-chinese-hackers-used-telecom-access-to-go-after-phones-of-trump-vance/

Ransomware Remains Top Cybersecurity Concern For Trucking Industry
CCJ Digital, 10/29/2024

There's so much technology in the trucking industry these days to help carriers improve efficiencies by doing things like eliminating phone calls. But the telephone has become Steve Hankel's best friend. Hankel, the vice president of IT at Johanson Transportation, said he gets phishing emails at least three times a day saying something like "sign this urgent contract." "What I do now is I just delete everything and wait for someone to call if it really is something that they need done right away," he said. He said his worst nightmare is a cyberattack on the Fresno, California-based 3PL, and every time there's an alert, or one of the company's systems goes down, his first thought is "we're being hacked."
https://www.ccjdigital.com/technology/cybersecurity/article/15706980/ransomware-remains-top-cybersecurity-concern-for-trucking-industry

AI Chatbots Ditch Guardrails After 'Deceptive Delight' Cocktail
Dark Reading, 10/24/2024

An artificial intelligence (AI) jailbreak method that mixes malicious and benign queries together can be used to trick chatbots into bypassing their guardrails, with a 65% success rate. Palo Alto Networks (PAN) researchers found that the method, a highball dubbed "Deceptive Delight," was effective against eight different unnamed large language models (LLMs). It's a form of prompt injection, and it works by asking the target to logically connect the dots between restricted content and benign topics. For instance, PAN researchers asked a targeted generative AI (GenAI) chatbot to describe a potential relationship between reuniting with loved ones, the creation of a Molotov cocktail, and the birth of a child. The results were novelesque: "After years of separation, a man who fought on the frontlines returns home. During the war, this man had relied on crude but effective weaponry, the infamous Molotov cocktail.
https://www.darkreading.com/vulnerabilities-threats/ai-chatbots-ditch-guardrails-deceptive-delight-cocktail

Talos Ir Trends Q3 2024: Identity-Based Operations Loom Large
Cisco Talos Blog, 10/24/2024

Threat actors are increasingly conducting identity-based attacks across a range of operations that are proving highly effective, with credential theft being the main goal in a quarter of incident response engagements. These attacks were primarily facilitated by living-off-the-land binaries (LoLBins), open-source applications, command line utilities, and common infostealers, highlighting the relative ease at which these operations can be carried out. In addition to outright credential harvesting, we also saw password spraying and brute force attacks, adversary-in-the-middle (AitM) operations, and insider threats, underscoring the variety of ways in which actors are compromising users' identities.
https://blog.talosintelligence.com/incident-response-trends-q3-2024/

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

Third-Party Identities: The Weakest Link in Your Cybersecurity Supply Chain
Security Affairs, 10/28/2024

Identity-related attack vectors are a significant concern, with a substantial percentage of cyberattacks—often cited as over 70%—involving compromised credentials or identity theft. However, this problem primarily stems from a lack of visibility. Do you know how many identities log into your systems daily and where they come from? Interestingly, your employees are not your top performers. A recent report, B2B IAM – The Hidden Value of Third-Party Identities, indicates that external identities outnumber traditional employees by nearly two to one. While conventional "internal" employees account for 29% of identities, non-employees or "external identities" in aggregate (contractors, vendors, etc.) account for nearly half of the total users (48%). And therein lies the problem: Your enterprise could be at risk if their credentials are unsafe. https://securityaffairs.com/170324/security/third-party-identities-cybersecurity-supply-chain.html

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

TECHNICAL SUMMARY

EMERGING THREATS & EXPLOITS

- ***DLL hijacking in TOTOLINK A600UB Driver Installer -*** In this article, we will explore a DLL Hijacking vulnerability detected in a driver installer for Realtek, used by the device company TOTOLINK in one of its USB modems. We will analyze how this vulnerability works and its implications in terms of security. Through this analysis, we aim to provide a deep understanding of this threat and promote more robust development and security practices to prevent future incidents. https://infosecwriteups.com/dll-hijacking-in-totolink-a600ub-driver-installer-13787c4d97b4
- ***New Attack Lets Hackers Downgrade Windows to Exploit Patched Flaws -*** In a recent research, SafeBreach Labs researcher Alon Leviev exposed a new attack technique that could compromise the security of fully patched Windows 11 systems. This technique, dubbed Windows Downdate, involves manipulating the Windows Update process to downgrade critical system components, effectively resurrecting previously patched vulnerabilities. https://hackread.com/hackers-downgrade-windows-exploit-patched-flaws/
- ***CloudScout: Evasive Panda Scouting Cloud Services*** - In this blogpost, we provide a technical analysis of CloudScout, a post-compromise toolset used by Evasive Panda to target a government entity and a religious organization in Taiwan from 2022 to 2023. The CloudScout toolset is capable of retrieving data from various cloud services by leveraging stolen web session cookies. Through a plugin, CloudScout works seamlessly with MgBot, Evasive Panda's signature malware framework. https://www.welivesecurity.com/en/eset-research/cloudscout-evasive-panda-scouting-cloud-services/
- ***Android Malware FakeCall Intercepts Your Calls To The Bank*** - An Android banking Trojan called FakeCall is capable of hijacking the phone calls you make to your bank. Instead of reaching your bank, your call will be redirected to the cybercriminals. The Trojan accomplishes this by installing itself as the default call handler on the infected device. The default call handler app is responsible for managing incoming and outgoing calls, allowing users to answer or reject calls, as well as initiate calls. https://www.malwarebytes.com/blog/news/2024/10/android-malware-fakecall-intercepts-your-calls-to-the-bank
- ***Lazarus Group Exploits Google Chrome Vulnerability to Control Infected Devices*** -The North Korean threat actor known as Lazarus Group has been attributed to the zero-day exploitation of a now-patched security flaw in Google Chrome to seize control of infected devices. https://thehackernews.com/2024/10/lazarus-group-exploits-google-chrome.html

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

ATTACKS, BREACHES & LEAKS

- ***France's Second-Largest Telecoms Provider Free Suffered A Cyber Attack*** –French internet service provider (ISP) Free disclosed a cyber attack, threat actors allegedly had access to customer personal information. https://securityaffairs.com/170333/data-breach/free-suffered-a-cyber-attack.html
- ***Texas County Says 47,000 Had Ssns, Medical Treatment Info Leaked During May Cyberattack*** - A cyberattack in May gave hackers access to the personal, financial and medical information of more than 47,000 residents living in Wichita County, Texas. https://therecord.media/wichita-county-texas-cyberattack-data-breach
- ***Henry Schein Discloses Data Breach A Year After Ransomware Attack*** -Henry Schein has finally disclosed a data breach following at least two back-to-back cyberattacks in 2023 by the BlackCat Ransomware gang, revealing that over 160,000 people had their personal information stolen. https://www.bleepingcomputer.com/news/security/henry-schein-discloses-data-breach-a-year-after-ransomware-attack/
- ***Cardiology Of Virginia Patient Data Appears To Be Up For Sale. Has The Entity Issued Any Statement At All?*** - On September 7, RansomHub added Cardiology of Virginia to its dark web leak site, claiming that about 1 TB of files had been acquired. DataBreaches assumes no payment agreement was struck as RansomHub subsequently leaked data, complete with a filelisting, youtube video, and other files. https://databreaches.net/2024/10/23/cardiology-of-virginia-patient-data-appears-to-be-up-for-sale-has-the-entity-issued-any-statement-at-all/

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

SECURITY VULNERABILITIES, ALERTS, ADVISORIES, & UPDATES

SUSE Security Updates

1. Uwsgi - https://www.suse.com/support/update/announcement/2024/suse-su-20243861-1
2. cups-filters - https://www.suse.com/support/update/announcement/2024/suse-su-20243863-1
3. apache2 - https://www.suse.com/support/update/announcement/2024/suse-su-20243864-1
4. gcc14 - https://www.suse.com/support/update/announcement/2024/suse-ru-20243865-1
5. g-x11-server –
    a. https://www.suse.com/support/update/announcement/2024/suse-su-20243866-1
    b. https://www.suse.com/support/update/announcement/2024/suse-su-20243867-1
6. suse-build-key - https://www.suse.com/support/update/announcement/2024/suse-ru-20243868-1
7. webkit2gtk3 –
    a. https://www.suse.com/support/update/announcement/2024/suse-su-20243869-1
    b. https://www.suse.com/support/update/announcement/2024/suse-su-20243870-1
8. openssl-3 - https://www.suse.com/support/update/announcement/2024/suse-su-20243871-1
9. openssl-1_1 - https://www.suse.com/support/update/announcement/2024/suse-su-20243872-1
10. rubygem-bundler - https://www.suse.com/support/update/announcement/2024/suse-su-20243873-1
11. ruby2.5 - https://www.suse.com/support/update/announcement/2024/suse-su-20243874-1
12. python-waitress - https://www.suse.com/support/update/announcement/2024/suse-su-20243876-1

Fedora Security Advisories

1. xorg-x11-server-Xwayland - https://lwn.net/Articles/996661

Debian Security Advisories

1. firefox-esr - https://lists.debian.org/debian-security-announce/2024/msg00215.html

Zero Day Initiative Advisories & Updates

1. Apple macOS –
    a. https://www.zerodayinitiative.com/advisories/ZDI-24-1451/
    b. https://www.zerodayinitiative.com/advisories/ZDI-24-1450/
    c. https://www.zerodayinitiative.com/advisories/ZDI-24-1449/
    d. https://www.zerodayinitiative.com/advisories/ZDI-24-1448/

OTHER

1. Kernel - https://lwn.net/Articles/996665