Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

Daily Open-Source Cyber Report

November 15, 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

Interdependencies and Collective Defense

Due to the various dependencies and interdependencies between infrastructure sectors, a disruption or breakdown in any one sector could create cascading effects that impact other sectors, which, in turn, affects still more sectors. There are many ways you and your organization can take part in our collective defense. To learn more, visit: https://www.cisa.gov/

Additional Resource:
Preparedness Planning for Your Business; Ready.gov https://www.ready.gov/business

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

AT-A-GLANCE

Executive News

- DHS Issues Internal Comms Guidance Amid Telecom Breach Investigation
- FBI: Spike in Hacked Police Emails, Fake Subpoenas
- Palo Alto Networks Emphasizes Hardening Guidance
- Pro-Russian Hacktivists Target South Korea as North Korea Joins Ukraine War
- Spot Rates Break Out Ahead Of Holidays
- Breaking Down Earth Estries' Persistent TTPs in Prolonged Cyber Operations
- The Biggest Inhibitor of Cybersecurity: The Human Element

Emerging Threats & Vulnerabilities

- Hello Again, Fakebat: Popular Loader Returns After Months-Long Hiatus
- Industrial Companies In Europe Targeted With Guloader
- Veeam Backup & Replication Exploit Reused In New Frag Ransomware Attack
- HPE Warns Of Critical RCE Flaws In Aruba Networking Access Points
- Androxgh0st Botnet Integrates Mozi, Expands Attacks on IoT Vulnerabilities

Attacks, Breaches, & Leaks

- 122 Million People’s Business Contact Info Leaked By Data Broker
- Karl Malone Toyota Data Breach
- A Cyberattack On Payment Systems Blocked Cards Readers Across Stores And Gas Stations In Israel
- Ahold Delhaize Cybersecurity Incident Impacts Giant Food, Hannaford
- Authority: Up To 300k People Impacted In City Of Helsinki’s Massive Data Breach

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

DHS Issues Internal Comms Guidance Amid Telecom Breach Investigation
Next Gov, 11/11/2024

The Department of Homeland Security's chief information officer issued internal guidance to all agency staff on Friday reminding employees to only use DHS-assigned devices for official business, according to email text obtained by Nextgov/FCW. The email was sent amid an ongoing governmentwide investigation into a Chinese infiltration of U.S. telecommunications systems. DHS CIO Eric Hysen also advised staff to only use Microsoft Teams to communicate whenever possible and to be cautious about phone calls and SMS text messages. The notice comes amid recent sweeping Chinese infiltration into a slew of telecommunications firms and infrastructure tied to court-authorized wiretap requests via a group dubbed Salt Typhoon, though the email does not explicitly mention the hacking collective or its recent intrusions. https://www.nextgov.com/cybersecurity/2024/11/dhs-issues-internal-comms-guidance-amid-telecom-breach-investigation/400956/

FBI: Spike in Hacked Police Emails, Fake Subpoenas
Krebson Security, 11/9/2024

The Federal Bureau of Investigation (FBI) is urging police departments and governments worldwide to beef up security around their email systems, citing a recent increase in cybercriminal services that use hacked police email accounts to send unauthorized subpoenas and customer data requests to U.S.-based technology companies. In an alert (PDF) published this week, the FBI said it has seen un uptick in postings on criminal forums regarding the process of emergency data requests (EDRs) and the sale of email credentials stolen from police departments and government agencies.
https://krebsonsecurity.com/2024/11/fbi-spike-in-hacked-police-emails-fake-subpoenas/

Palo Alto Networks Emphasizes Hardening Guidance
CISA, 11/15/2024

Palo Alto Networks (PAN) has updated their informational bulletin, noting they "observed threat activity exploiting an unauthenticated remote command execution vulnerability against a limited number of firewall management interfaces which are exposed to the Internet." CISA continues to urge users and administrators to review the following for more information, follow PAN's guidance for hardening network devices, review PAN's instruction for accessing organization's scan results for internet-facing management interfaces, and take immediate action if required https://www.cisa.gov/news-events/alerts/2024/11/13/palo-alto-networks-emphasizes-hardening-guidance

Pro-Russian Hacktivists Target South Korea as North Korea Joins Ukraine War
Infosecurity Magazine, 11/8/2024

Russian-associated cyber-attacks on South Korea have ramped up following the deployment of North Korean troops in Ukraine, South Korea's President's Office has warned. The activity by pro-Kremlin groups has primarily been distributed denial-of-service (DDoS) attacks against government websites and private companies, which the Seoul government is actively responding to. The President's Office said that access to the websites of some institutions have been temporarily delayed or cut off as a result of the attacks, but no other damage has been observed. “Cyber-attacks by pro-Russian hacktivist groups against South Korea have been intermittent in the past, but since North Korea's deployment to Russia and its entry into the war in Ukraine, attacks have become more frequent,” the office warned.
https://www.infosecurity-magazine.com/news/russian-hacktivits-south-korea/

Spot Rates Break Out Ahead Of Holidays
Freight Waves, 11/9/2024

Nationwide dry van spot rates minus the influence of fuel jumped 5% last week as carriers rejected contracted truckload tenders at the second-fastest pace of the year, prompting FreightWaves CEO and founder Craig Fuller to call an end to the Great Freight Recession. The National Truckload Index Linehaul Only (NTIL) measures the average spot rate for dry van loads moving more than 250 miles excluding the total estimated cost of fuel. The NTIL has been trending higher over the past year and a half but has moved erratically, as is the nature of commodities negotiated on a daily basis.
https://www.freightwaves.com/news/spot-rates-break-out-ahead-of-holidays

Breaking Down Earth Estries' Persistent TTPs in Prolonged Cyber Operations
Trend Micro, 11/8/2024

In early 2023, we published a blog entry on campaigns targeting governments and the tech industry from Earth Estries (aka Salt Typhoon), a high-level threat actor that has been active since at least 2020. In this report, we analyze two distinct attack chains by the group that demonstrates the varied tactics, techniques, and tools that they use to compromise targeted systems. There are some commonalities between the two attack chains, like the abuse of vulnerable attack surfaces such as Microsoft Exchange servers and network adapter management tools. However, there are also significant differences. The first chain employs PsExec and WMI command-line (WMIC) for lateral movement, using tools such as Cobalt Strike, Trillclient, Hemigate, and Crowdoor, which are delivered via CAB file packages. The second chain showcases a different approach, using malware such as Zingdoor, Cobalt Strike, and SnappyBee, as well as utility tools like PortScan and NinjaCopy, which are delivered via curl downloads.
https://www.trendmicro.com/en_us/research/24/k/breaking-down-earth-estries-persistent-ttps-in-prolonged-cyber-o.html

The Biggest Inhibitor of Cybersecurity: The Human Element
Cyber Scoop, 11/6/2024

Global spending on information security is projected to reach $212 billion in 2025, reflecting a 15.1% increase from 2024, according to Gartner's latest forecast. Despite this surge in investment, breaches remain rampant, as seen in recent incidents such as the ransomware attack on Change Healthcare and a brute-force campaign exploiting vulnerabilities in various Cisco products. While technology plays an essential role in fortifying organizations against cyber threats, adversaries continue to exploit the weakest link in the defense chain: the human element. According to the 2024 Verizon Business Data Breach Investigations Report (DBIR), the human element was a component of 68% of all data breaches. It is often said that the most sophisticated security controls can be undermined by a single click from an uninformed or careless employee. https://www.securityweek.com/the-biggest-inhibitor-of-cybersecurity-the-human-element/

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

TECHNICAL SUMMARY

EMERGING THREATS & EXPLOITS

- ***Hello Again, Fakebat: Popular Loader Returns After Months-Long Hiatus*** - The web browser, and search engines in particular, continue to be a popular entry point to deliver malware to users. While we noted a decrease in loaders distributed via malvertising for the past 3 months, today's example is a reminder that threat actors can quickly switch back to tried and tested methods. https://www.malwarebytes.com/blog/news/2024/11/hello-again-fakebat-popular-loader-returns-after-months-long-hiatus
- ***Industrial Companies In Europe Targeted With Guloader*** - A recent spear-phishing campaign targeting industrial and engineering companies in Europe was aimed at saddling victims with the popular GuLoader downloader and, ultimately, a remote access trojan that would permit attackers to steal information from and access compromised computers whenever they wish. https://www.helpnetsecurity.com/2024/11/07/industrial-europe-spear-phishing-guloader/
- ***Veeam Backup & Replication Exploit Reused In New Frag Ransomware Attack(LL)*** **-** In mid-October, Sophos researchers warned that ransomware operators are exploiting the critical vulnerability CVE-2024-40711 in Veeam Backup & Replication to create rogue accounts and deploy malware. https://securityaffairs.com/170717/malware/veeam-backup-replication-flaw-frag-ransomware.html
- ***HPE Warns Of Critical RCE Flaws In Aruba Networking Access Points*** **–** Hewlett Packard Enterprise (HPE) released updates for Instant AOS-8 and AOS-10 software to address two critical vulnerabilities in Aruba Networking Access Points. https://www.bleepingcomputer.com/news/security/hpe-warns-of-critical-rce-flaws-in-aruba-networking-access-points/
- ***Androxgh0st Botnet Integrates Mozi, Expands Attacks on IoT Vulnerabilities*** **-** CloudSEK reports that the Androxgh0st botnet has integrated with the Mozi botnet and exploits a wide range of vulnerabilities in web applications and IoT devices. Learn about the specific vulnerabilities being targeted, the techniques used by the attackers, and how to protect your systems from this evolving threat. https://hackread.com/androxgh0st-botnet-integrate-mozi-iot-vulnerabilities/

ATTACKS, BREACHES & LEAKS

- ***122 Million People's Business Contact Info Leaked By Data Broker -*** A data broker has confirmed a business contact information database containing 132.8 million records has been leaked online. In February, 2024, a cybercriminal offered the records for sale on a data breach forum claiming the information came from pureincubation[.]com. https://www.malwarebytes.com/blog/news/2024/11/122-million-peoples-business-contact-info-leaked-by-data-broker
- ***Karl Malone Toyota Data Breach*** - Karl Malone offers Toyota dealership, selling new and pre-owned vehicles. https://www.breachsense.com/breaches/karl-malone-toyota-data-breach/
- ***A Cyberattack On Payment Systems Blocked Cards Readers Across Stores And Gas Stations In Israel*** - The Jerusalem Post reported that thousands of credit card readers across at gas stations and supermarket chains in Israel stopped working on Sunday morning following an alleged DDoS attack that hit the company responsible for the operations of the devices. https://securityaffairs.com/170823/hacking/cyberattack-payment-systems-israel.html
- ***Ahold Delhaize Cybersecurity Incident Impacts Giant Food, Hannaford*** - Giant Food pharmacies and Hannaford supermarkets are among the impacted brands that have reported network issues as result of the incident, but other brands might be affected as well. https://www.securityweek.com/ahold-delhaize-cybersecurity-incident-impacts-giant-food-hannaford/
- ***Authority: Up To 300k People Impacted In City Of Helsinki's Massive Data Breach -*** The Safety Investigation Authority of Finland (Otkes) is continuing an investigation of a massive data breach that targeted the City of Helsinki last spring. Otkes said investigators have already collected more than 90 percent of the data involved in the exceptionally large-scale breach. https://databreaches.net/2024/11/15/authority-up-to-300k-people-impacted-in-city-of-helsinkis-massive-data-breach/

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

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

SECURITY VULNERABILITIES, ALERTS, ADVISORIES, & UPDATES

SUSE Security Updates

1. Drbd - https://www.suse.com/support/update/announcement/2024/suse-ru-20243991-1
2. Libvdpau - https://www.suse.com/support/update/announcement/2024/suse-ru-20243992-1
3. rabbitmq-c - https://www.suse.com/support/update/announcement/2024/suse-ru-20243993-1
4. ucode-intel - https://www.suse.com/support/update/announcement/2024/suse-su-20243995-1
5. python3-wxPython - https://www.suse.com/support/update/announcement/2024/suse-su-20243997-1
6. glib2 - https://www.suse.com/support/update/announcement/2024/suse-su-20243998-1

Fedora Security Advisories

1. krb5 –
   a. https://lwn.net/Articles/998276
   b. https://lwn.net/Articles/998276

Red Hat Security Advisories

1. Apache Camel 4.4.4 - https://access.redhat.com/errata/RHSA-2024:9806