Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

Daily Open-Source Cyber Report

November 26, 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

Training and Exercises

Training and exercise improve security and resilience. CISA Tabletop Exercise Packages (CTEPs) are a comprehensive set of resources designed to assist stakeholders in conducting their own exercises. Partners can use CTEPs to initiate discussions within their organizations about their ability to address a variety of threat scenarios. Each package is customizable and includes template exercise objectives, scenarios, and discussion questions, as well as a collection of references and resources. Available scenarios cover a broad array of physical security and cybersecurity topics, including natural disasters, pandemics, civil disturbances, vehicle ramming, active assailants, Improvised Explosive Devices (IEDs), Unmanned Aircraft Systems (UAS), insider threats, ransomware, phishing, Industrial Control System (ICS) compromise, and cyber-physical convergence. CTEPs also provide scenario and module questions to discuss pre-incident information and intelligence sharing, incident response, and post-incident recovery.
https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

AT-A-GLANCE

Executive News

- Homeland Security Department Releases Framework for Using AI in Critical Infrastructure
- Alleged Russian Phobos Ransomware Administrator Extradited To U.S., In Custody
- U.S. Agencies Urged to Combat Growing Chinese Cyberthreat
- Fake Discount Sites Exploit Black Friday to Hijack Shopper Information
- Phishing Emails Increasingly Use SVG Attachments To Evade Detection
- Cybersecurity Training Is Crucial
- Why Shadow APIs Provide A Defenseless Path For Threat Actors

Emerging Threats & Vulnerabilities

- Inside Water Barghest's Rapid Exploit-to-Market Strategy for IoT Devices
- Mozilla 0Din Warns of ChatGPT Sandbox Flaws Enabling Python Execution
- Oracle patches exploited Agile PLM vulnerability (CVE-2024-21287)
- VMware Discloses Exploitation of Hard-to-Fix vCenter Server Flaw
- New Stealthy BabbleLoader Malware Spotted Delivering WhiteSnake and Meduza Stealers

Attacks, Breaches, & Leaks

- Hacker Obtained Documents Tied To Lawsuit Over Matt Gaetz's Sexual Misconduct Allegations
- U.S. and UK Military Social Network "Forces Penpals" Exposes SSN, PII Data
- Yakuza Victim Data Leaked in Japanese Agency Attack
- Hackers breach U.S. firm over Wi-Fi from Russia in 'Nearest Neighbor Attack'

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

EXECUTIVE NEWS

Homeland Security Department Releases Framework for Using AI in Critical Infrastructure
Security Week, 11/15/2024

Private industry would have to adopt and implement the guidelines announced by the Homeland Security Department, which were developed in consultation with the department's advisory Artificial Intelligence Safety and Security Board. Homeland Security Secretary Alejandro Mayorkas told reporters that "we intend the framework to be, frankly, a living document and to change as developments in the industry change as well." The framework recommends that AI developers evaluate potentially dangerous capabilities in their products, ensure their products align with "human-centric values" and protect users' privacy. The cloud-computing infrastructure would need to vet hardware and software suppliers and protect the physical security of data centers. https://www.securityweek.com/homeland-security-department-releases-framework-for-using-ai-in-critical-infrastructure/

Alleged Russian Phobos Ransomware Administrator Extradited To U.S., In Custody
Cyber Scoop, 11/18/2024

A Russian man who allegedly served as an administrator of the Phobos ransomware that's extorted millions of dollars from more than a thousand victims is in U.S. custody, the Justice Department said Monday. South Korea extradited Evgenii Ptitsyn, 42, to the United States for a court appearance Nov. 4, according to a news release about an unsealed 13-count indictment. The Phobos ransomware has extorted over $16 million from more than 1,000 victims worldwide, including schools, hospitals, government agencies and large corporations, DOJ said. The department chalked up the arrest to international team-ups. https://cyberscoop.com/alleged-russian-phobos-ransomware-administrator-extradited-to-u-s-in-custody/

U.S. Agencies Urged to Combat Growing Chinese Cyberthreat
Bleeping Computer, 11/19/2024

Cybersecurity experts called on key federal departments to do more to proactively combat escalating cyberthreats from China, including enhanced public-private collaboration and increased investments in threat intelligence, critical infrastructure resilience and advanced defensive technologies. Threat actors linked to Beijing are intensifying sophisticated espionage campaigns and hacking operations targeting U.S. critical infrastructure and top officials, cybersecurity experts testified during a Senate Judiciary Committee hearing Tuesday. https://www.govinfosecurity.com/us-agencies-urged-to-combat-growing-chinese-cyberthreat-a-26858

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

Fake Discount Sites Exploit Black Friday to Hijack Shopper Information
The Hacker News, 11/18/2024

A new phishing campaign is targeting e-commerce shoppers in Europe and the United States with bogus pages that mimic legitimate brands with the goal of stealing their personal information ahead of the Black Friday shopping season. "The campaign leveraged the heightened online shopping activity in November, the peak season for Black Friday discounts. The threat actor used fake discounted products as phishing lures to deceive victims into providing their Cardholder Data (CHD) and Sensitive Authentication Data (SAD) and Personally Identifiable Information (PII)," EclecticIQ said. The activity, first observed in early October 2024, has been attributed with high confidence to a Chinese financially motivated threat actor codenamed SilkSpecter. Some of the impersonated brands include IKEA, L.L.Bean, North Face, and Wayfare. https://thehackernews.com/2024/11/fake-discount-sites-exploit-black.html

Phishing Emails Increasingly Use SVG Attachments To Evade Detection
Bleeping Computer, 11/17/2024

Threat actors increasingly use Scalable Vector Graphics (SVG) attachments to display phishing forms or deploy malware while evading detection. Most images on the web are JPG or PNG files, which are made of grids of tiny squares called pixels. Each pixel has a specific color value, and together, these pixels form the entire image. SVG, or Scalable Vector Graphics, displays images differently, as instead of using pixels, the images are created through lines, shapes, and text described in textual mathematical formulas in the code. For example, the following text will create a rectangle, a circle, a link, and some text: https://www.bleepingcomputer.com/news/security/phishing-emails-increasingly-use-svg-attachments-to-evade-detection/

Cybersecurity Training Is Crucial
Fleet Owner, 11/21/2024

In today's digital age, cybersecurity is not an IT issue; it's a business issue. Cyberattacks can bring your operations to a grinding halt, impacting revenue and reputation and eroding customer trust. With connected vehicles, telematics, and back-office digitization, the trucking industry is more exposed than ever. Investing in cybersecurity awareness training that's tailored to the needs of every part of your team, from back-office staff to drivers to maintenance crews, is critical. When all employees are trained in cybersecurity basics, the risk of human error leading to a cyber incident is significantly reduced. Each role within your organization is faced with unique challenges, threats, and levels of technology exposure, so this training should be personalized to ensure it is effective. https://www.fleetowner.com/perspectives/ideaxchange/article/55243147/cybersecurity-training-is-crucial-for-trucking

Why Shadow APIs Provide A Defenseless Path For Threat Actors
Security Boulevard, 11/19/2024

In API security, one of the least visible and most dangerous issues today is the prevalence of Shadow APIs. Understanding the threats posed by these hidden APIs is critical for those new to API security research and testing. They can easily slip under the radar of even the most diligent security teams, providing a clear path for threat actors to infiltrate systems and compromise sensitive data. This post explores Shadow APIs, their security risks, and how to start defending against them. Simply put, Shadow APIs are undocumented or unknown APIs that exist within a company's infrastructure but aren't accounted for in official documentation. https://securityboulevard.com/2024/11/why-shadow-apis-provide-a-defenseless-path-for-threat-actors/

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

TECHNICAL SUMMARY

EMERGING THREATS & EXPLOITS

- ***Inside Water Barghest's Rapid Exploit-to-Market Strategy for IoT Devices*** - There is a big incentive for both espionage motivated actors and financially motivated actors to set up proxy botnets. These can serve as an anonymization layer, which can provide plausibly geolocated IP addresses to scrape contents of websites, access stolen or compromised online assets, and launch cyber-attacks. https://www.trendmicro.com/en_us/research/24/k/water-barghest.html
- ***Mozilla 0Din Warns of ChatGPT Sandbox Flaws Enabling Python Execution*** - Mozilla's 0Din uncovers critical flaws in ChatGPT's sandbox, allowing Python code execution and access to internal configurations. OpenAI has addressed only one of five issues. https://hackread.com/mozilla-0din-chatgpt-sandbox-flaws-python-execution/
- ***Oracle patches exploited Agile PLM vulnerability (CVE-2024-21287) –*** Oracle has released a security patch for CVE-2024-21287, a remotely exploitable vulnerability in the Oracle Agile PLM Framework that is, according to Tenable researchers, being actively exploited by attackers. https://www.helpnetsecurity.com/2024/11/19/cve-2024-21287/
- ***VMware Discloses Exploitation of Hard-to-Fix vCenter Server Flaw –*** The difficult-to-fix vulnerability, first revealed at a Chinese hacking contest five months ago, is now being exploited in the wild, the company confirmed on Monday. https://www.securityweek.com/vmware-discloses-exploitation-of-hard-to-fix-vcenter-server-flaw/
- ***New Stealthy BabbleLoader Malware Spotted Delivering WhiteSnake and Meduza Stealers*** - Cybersecurity researchers have shed light on a new stealthy malware loader called BabbleLoader that has been observed in the wild delivering information stealer families such as WhiteSnake and Meduza. https://thehackernews.com/2024/11/new-stealthy-babbleloader-malware.html

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

ATTACKS, BREACHES & LEAKS

- ***Hacker Obtained Documents Tied To Lawsuit Over Matt Gaetz's Sexual Misconduct Allegations*** **-** A hacker allegedly accessed a file containing testimony from a woman claiming she had sex with Matt Gaetz when she was 17, sparking controversy. https://securityaffairs.com/171207/security/matt-gaetzs-sexual-misconduct-allegations-doc-compromised.html
- ***U.S. and UK Military Social Network "Forces Penpals" Exposes SSN, PII Data*** - Forces Penpals, a social network for US and UK military personnel, exposed the sensitive data of 1.1M users, including SSNs, personal details, and proof of service. Learn about the incident and its possible impact. https://hackread.com/us-uk-military-forces-penpals-exposes-ssn-pii-data/
- ***Yakuza Victim Data Leaked in Japanese Agency Attack*** **-** Japan's web of ruthless Yakuza organized crime syndicates continues to operate, threatening the country's citizens with everything from extortion to gangland murders. Local agencies within communities are set up to help those who get involved with gangsters — but unfortunately, one of them has been hacked, potentially leading to physical safety consequences for the victims. https://www.darkreading.com/cyberattacks-data-breaches/yakuza-victim-data-leaked-japanese-attack
- ***Hackers breach U.S. firm over Wi-Fi from Russia in 'Nearest Neighbor Attack'*** - Russian state hackers APT28 (Fancy Bear/Forest Blizzard/Sofacy) breached a U.S. company through its enterprise WiFi network while being thousands of miles away, by leveraging a novel technique called "nearest neighbor attack." https://www.bleepingcomputer.com/news/security/hackers-breach-us-firm-over-wi-fi-from-russia-in-nearest-neighbor-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. Array Networks - https://www.cve.org/CVERecord?id=CVE-2023-28461
2. Schneider Electric –
    a. https://www.cisa.gov/news-events/ics-advisories/icsa-24-331-01
    b. https://www.cisa.gov/news-events/ics-advisories/icsa-24-331-02
    c. https://www.cisa.gov/news-events/ics-advisories/icsa-24-331-03
3. Hitachi Energy –
    a. https://www.cisa.gov/news-events/ics-advisories/icsa-24-331-04
    b. https://www.cisa.gov/news-events/ics-advisories/icsa-24-331-05
4. Philips - https://www.cisa.gov/news-events/ics-medical-advisories/icsma-24-200-01

SUSE Security Updates

1. ucode-intel - https://www.suse.com/support/update/announcement/2024/suse-su-20244053-1
2. javapackages-tools, xmlgraphics-batik, xmlgraphics-commons, xmlgraphics-fop - https://www.suse.com/support/update/announcement/2024/suse-su-20244054-1
3. Jackson - https://www.suse.com/support/update/announcement/2024/suse-ru-20244055-1
4. Apache2 - https://www.suse.com/support/update/announcement/2024/suse-ru-20244056-1
5. selinux-policy - https://www.suse.com/support/update/announcement/2024/suse-ru-20244057-1
6. hawtjni-runtime - https://www.suse.com/support/update/announcement/2024/suse-ru-20244058-1
7. httpcomponents-asyncclient - https://www.suse.com/support/update/announcement/2024/suse-ru-20244059-1
8. ocl-icd - https://www.suse.com/support/update/announcement/2024/suse-ru-20244060-1
9. rubygem-nokogiri - https://www.suse.com/support/update/announcement/2024/suse-ru-20244061-1
10. vexctl - https://www.suse.com/support/update/announcement/2024/suse-ru-20244064-1
11. crypto-policies - https://www.suse.com/support/update/announcement/2024/suse-ru-20244065-1
12. openssh - https://www.suse.com/support/update/announcement/2024/suse-ru-20244067-1
13. automake - https://www.suse.com/support/update/announcement/2024/suse-ru-20244068-1
14. yast2-iscsi-client - https://www.suse.com/support/update/announcement/2024/suse-ru-20244069-1

Fedora Security Advisories

1. Cobbler –
    a. https://lwn.net/Articles/999724
    b. https://lwn.net/Articles/999725
2. Chromium - https://lwn.net/Articles/999723
3. libsoup3 - https://lwn.net/Articles/999727

Check Point Security Advisories

1. Digium Asterisk - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-1067.html
2. Zyxel - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2023-1538.html
3. Apache - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-0557.html

Red Hat Security Advisories

1. OpenShift Virtualization 4.13.11 Images - https://access.redhat.com/errata/RHSA-2024:10389
2. Red Hat JBoss Enterprise - https://access.redhat.com/errata/RHSA-2024:10385
3. Tuned - https://access.redhat.com/errata/RHSA-2024:10384

Ubuntu Security Notices

1. RapidJSON - https://ubuntu.com/security/notices/USN-7125-1
2. Needrestart - https://ubuntu.com/security/notices/USN-7117-2

Oracle Linux Security Update

1. Kernel –
    a. https://lwn.net/Articles/999728
    b. https://lwn.net/Articles/999730
    c. https://lwn.net/Articles/999729

OTHER

1. Google Chrome –
    a. https://chromereleases.googleblog.com/2024/11/long-term-support-channel-update-for.html
    b. https://chromereleases.googleblog.com/2024/11/chrome-stable-for-ios-update_12.html
    c. https://chromereleases.googleblog.com/2024/11/extended-stable-updates-for-desktop.html
    d. https://chromereleases.googleblog.com/2024/11/stable-channel-update-for-desktop_12.html
    e. https://chromereleases.googleblog.com/2024/11/stable-channel-update-for-chromeos_12.html