Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

Daily Open-Source Cyber Report

December 4, 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 and Partners Release Joint Guidance on PRC-Affiliated Threat Actor Compromising Networks of Global Telecommunications Providers
- Major Cybercrime Operation Nets 1,006 Suspects
- Thai Police Arrested Chinese Hackers Involved In Sms Blaster Attacks
- At Least $100,000 In Transit Fare Revenue Lost From Cyberattack On Oahu Transit Services
- Here's How Simple It Is For Script Kiddies To Stand Up DDoS Services
- Digital Rail Solutions Are More Vital Than Ever
- Flying Under the Radar - Security Evasion Techniques

Emerging Threats & Vulnerabilities

- Guess Who's Back - The Return of ANEL in the Recent Earth Kasha Spear-phishing Campaign in 2024
- RomCom Hackers Chained Firefox And Windows Zero-Days To Deliver Backdoor
- CISA Urges Agencies to Patch Critical "Array Networks" Flaw Amid Active Attacks
- IBM Patches RCE Vulnerabilities in Data Virtualization Manager, Security SOAR
- New NachoVPN Attack Uses Rogue VPN Servers To Install Malicious Updates

Attacks, Breaches, & Leaks

- RansomHub Hits Belgian Manufacturer Potteau in Data Breach
- Energy Industry Contractor Englobal Corporation Discloses A Ransomware Attack
- Over 600,000 Records, Including Background Checks, Vehicle, and Property Records Exposed Online: SL Data Services/Propertyrec
- Zello Asks Users To Reset Passwords After Security Incident

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

EXECUTIVE NEWS

CISA and Partners Release Joint Guidance on PRC-Affiliated Threat Actor Compromising Networks of Global Telecommunications Providers
CISA, 12/3/2024

This guidance was crafted in response to a People's Republic of China (PRC)-affiliated threat actor's compromise of "networks of major global telecommunications providers to conduct a broad and significant cyber espionage campaign." The compromise of private communications impacted a limited number of individuals who are primarily involved in government or political activity. CISA and partners encourage network defenders and engineers of communications infrastructure, and other critical infrastructure organizations with on-premises enterprise equipment, to review and apply the provided best practices, including patching vulnerable devices and services, to reduce opportunities for intrusion. For more information on PRC state-sponsored threat actor activity, see CISA's People's Republic of China Cyber Threat. https://www.cisa.gov/news-events/alerts/2024/12/03/cisa-and-partners-release-joint-guidance-prc-affiliated-threat-actor-compromising-networks-global

Major Cybercrime Operation Nets 1,006 Suspects
Interpol, 11/26/2024

Authorities across 19 African countries have arrested 1,006 suspects and dismantled 134,089 malicious infrastructures and networks thanks to a joint operation by INTERPOL and AFRIPOL against cybercrime. Operation Serengeti (2 September - 31 October) targeted criminals behind ransomware, business email compromise (BEC), digital extortion and online scams - all identified as prominent threats in the 2024 Africa Cyber Threat Assessment Report. More than 35,000 victims were identified during the operation, with cases linked to nearly USD 193 million in financial losses worldwide. Information provided by participating countries of ongoing cases with INTERPOL fed into 65 Cyber Analytical Reports that were produced to ensure actions on the ground were intelligence-led and focused on the most significant actors. https://www.interpol.int/en/News-and-Events/News/2024/Major-cybercrime-operation-nets-1-006-suspects

Thai Police Arrested Chinese Hackers Involved In Sms Blaster Attacks
Security Affairs, 11/26/2024

Thai authorities arrested members of two Chinese cybercrime organizations, one of these groups carried out SMS blaster attacks. The crooks were driving through Bangkok's streets while sending hundreds of thousands of malicious SMS text messages to nearby cell phones. "One of these gangs had disguised themselves as a legitimate company to register phone numbers '02-xxxxxxx' used to deceive the public. Another using False Base Stations to send fake SMS messages to victims" states the Thai news outlet https://securityaffairs.com/171406/cyber-crime/sms-blaster-attacks-bangkok.html

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

At Least $100,000 In Transit Fare Revenue Lost From Cyberattack On Oahu Transit Services
Transit Talent, 11/27/2024

A crippling cyberattack that targeted TheBus and The -Handi-Van earlier this year wound up costing the city $100,000 or more in lost fare revenue, Honolulu officials indicate. Nearly a half-year later, Oahu Transit Services Inc., the private company that manages the city's bus and paratransit system, said it's still working on implementing cybersecurity measures to protect its fleet as well as its ridership. Over several days in mid-June, OTS said, thebus.org website, HEA (also known as Honolulu Estimated Arrival) and related GPS services were inoperable due to the cyberattack. The city Department of Transportation Services said on June 18 that there was a "cyber breach" and that OTS was working with the "proper authorities to investigate and handle the situation."
https://www.transittalent.com/articles/index.cfm?story=Lost_Fare_Revenue_In_Cyberattack_on_Oahu_Transit_Services_11-29-2024

Here's How Simple It Is For Script Kiddies To Stand Up DDoS Services
Cyber Scoop, 11/26/2024

A new report from Aqua Security highlights just how easy it is for an amateur-level hacker to set up malicious services that could in turn be weaponized by much-more skillful threat actors in the future. The cloud security company detailed in a report released Tuesday an operation to sell access to distributed denial-of-service (DDoS) tools on Telegram which was started by an apparent Russian threat actor known as "Matrix," citing the code commits from a GitHub account. The threat actor, which Aqua calls a "script kiddie," spent a year creating a botnet using a mashup of open-source hacking tools while exploiting old bugs and default credentials from routers, DVRs, and other internet-connected devices.
https://cyberscoop.com/russian-hacker-script-matrix-ddos-aqua/

Digital Rail Solutions Are More Vital Than Ever
Engineer Live, 11/25/2024

The rail sector faces several challenges, including ageing infrastructure, cybersecurity threats targeting critical systems, and pressure to reduce its carbon footprint while adapting to strict environmental regulations. A self-described 'next-gen technology leader', Eviden specialises in advanced computing, security, artificial intelligence (AI), cloud and digital platforms for a vast range of industries. Rail is a key sector for the company says Michael Todorovitsch - head of expert sales, transportation and logistics – as he walks me round Eviden's sizeable booth at Europe's largest rail show, Innotrans 2024. "Our main focus is on big data," he explains. "Of course, if you're talking about big data then you need to mention analytics, security, and last but not least, AI. Today, we're showing five different demo corners displaying the selected offerings we have especially for the rail industry, though our complete portfolio is much bigger." https://www.engineerlive.com/content/digital-rail-solutions-are-more-vital-ever

Flying Under the Radar - Security Evasion Techniques
The Hacker News, 11/25/2024

"I really like the saying that 'This is out of scope' said no hacker ever. Whether it's tricks, techniques or technologies, hackers will do anything to evade detection and make sure their attack is successful," says Etay Maor, Chief Security Strategist at Cato Networks and member of Cato CTRL. Phishing attacks have transformed significantly over the years. 15-20 years ago, simple phishing sites were sufficient for capturing the crown jewels of the time - credit card details. Today, attacks and defense methods have become much more sophisticated, as we'll detail below. "This is also the time where the "cat-and-mouse" attack-defense game began," says Tal Darsan, Security Manager and member of Cato CTRL.
https://thehackernews.com/2024/11/flying-under-radar-security-evasion.html

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

TECHNICAL SUMMARY

EMERGING THREATS & EXPLOITS

- ***Guess Who's Back - The Return of ANEL in the Recent Earth Kasha Spear-phishing Campaign in 2024 -*** This blog is a part of a blog series about Earth Kasha. Kindly refer to our blog about the previous campaigns, where we discussed the tactics and targets of Earth Kasha in detail, read here for a deeper understanding, https://www.trendmicro.com/en_us/research/24/k/return-of-anel-in-the-recent-earth-kasha-spearphishing-campaign.html
- ***RomCom Hackers Chained Firefox And Windows Zero-Days To Deliver Backdoor*** - Russia-aligned APT group RomCom was behind attacks that leveraged CVE-2024-9680, a remote code execution flaw in Firefox, and CVE-2024-49039, an elevation of privilege vulnerability in Windows Task Scheduler, as zero-days earlier this year. "Chaining together two zero-day vulnerabilities armed RomCom with an exploit that requires no user interaction," ESET researchers said. https://www.helpnetsecurity.com/2024/11/26/romcom-backdoor-cve-2024-9680-cve-2024-49039/
- ***CISA Urges Agencies to Patch Critical "Array Networks" Flaw Amid Active Attacks –*** The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Monday added a now-patched critical security flaw impacting Array Networks AG and vxAG secure access gateways to its Known Exploited Vulnerabilities (KEV) catalog following reports of active exploitation in the wild. https://thehackernews.com/2024/11/cisa-urges-agencies-to-patch-critical.html
- ***IBM Patches RCE Vulnerabilities in Data Virtualization Manager, Security SOAR –*** Tracked as CVE-2024-52899 (CVSS score of 8.5), the flaw in Data Virtualization Manager for z/OS could allow a remote, authenticated attacker to inject malicious JDBC URL parameters, which could lead to arbitrary code execution on the server. https://www.securityweek.com/ibm-patches-rce-vulnerabilities-in-data-virtualization-manager-security-soar/
- ***New NachoVPN Attack Uses Rogue VPN Servers To Install Malicious Updates*** **-** A set of vulnerabilities dubbed "NachoVPN" allows rogue VPN servers to install malicious updates when unpatched Palo Alto and SonicWall SSL-VPN clients connect to them. https://www.bleepingcomputer.com/news/security/new-nachovpn-attack-uses-rogue-vpn-servers-to-install-malicious-updates/

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

ATTACKS, BREACHES & LEAKS

- ***RansomHub Hits Belgian Manufacturer Potteau in Data Breach -*** Potteau, a leading Belgian company specializing in laboratory furniture and interior fittings, has fallen victim to a ransomware attack orchestrated by the notorious RansomHub group. The attack, discovered on November 12, 2024, has resulted in the exfiltration of 13 GB of sensitive data, with the cybercriminals threatening to release the information publicly. https://www.halcyon.ai/attacks/ransomhub-hits-belgian-manufacturer-potteau-in-data-breach
- ***Energy Industry Contractor Englobal Corporation Discloses A Ransomware Attack*** - A ransomware attack disrupted the operations of a major energy industry contractor, ENGlobal Corporation. Founded in 1985, ENGlobal Corporation designs automated control systems for commercial and government sectors, reporting $6 million in Q3 revenue and $18.4 million year-to-date.https://www.infosecurity-magazine.com/news/tmobile-salt-typhoon-did-not/
- ***Over 600,000 Records, Including Background Checks, Vehicle, and Property Records Exposed Online: SL Data Services/Propertyrec -*** Jeremiah Fowler reports finding another exposed database with a lot of personal information. This one may belong to SL Data Services, LLC, though Fowler notes that the folders inside it were named with separate website domains. “It appears that the company operates a network of an estimated 16 different websites, offering a range of information services,” WebsitePlanet reports. https://databreaches.net/2024/12/01/over-600000-records-including-background-checks-vehicle-and-property-records-exposed-online-sl-data-services-propertyrec/
- ***Zello Asks Users To Reset Passwords After Security Incident*** - Zello is warning customers to reset their passwords if their account was created before November 2nd in what appears to be another security breach. https://www.bleepingcomputer.com/news/security/zello-asks-users-to-reset-passwords-after-security-incident/

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. CyberPanel - https://www.cve.org/CVERecord?id=CVE-2024-51378

SUSE Security Updates

1. maven-shade-plugin - https://www.suse.com/support/update/announcement/2024/suse-ru-20244162-1
2. xen - https://www.suse.com/support/update/announcement/2024/suse-su-20244163-1
3. openldap2_5 - https://www.suse.com/support/update/announcement/2024/suse-ru-20244164-1
4. python –
    a. https://www.suse.com/support/update/announcement/2024/suse-su-20244165-1
    b. https://www.suse.com/support/update/announcement/2024/suse-su-20244166-1
    c. https://www.suse.com/support/update/announcement/2024/suse-su-20244169-1
5. Vim - https://www.suse.com/support/update/announcement/2024/suse-ru-20244168-1
6. webkit2gtk3 - https://www.suse.com/support/update/announcement/2024/suse-su-20244167-1

Mageia Security Advisories

1. qemu - http://advisories.mageia.org/MGASA-2024-0387.html
2. python-aiohttp - http://advisories.mageia.org/MGASA-2024-0388.html

Check Point Security Advisories

1. D-Link - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-1093.html
2. GL-iNet - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-1100.html
3. ProjectSend - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-1108.html
4. WebUI - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2023-1025.html
5. WordPress - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2014-2639.html
6. ManageEngine - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-1106.html
7. MacOS - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-1107.html

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

Drupal Security Advisories

1. Entity Form Steps - https://www.drupal.org/sa-contrib-2024-071
2. Minify JS - https://www.drupal.org/sa-contrib-2024-070
3. Download All Files - https://www.drupal.org/sa-contrib-2024-069
4. Pages Restriction Access - https://www.drupal.org/sa-contrib-2024-068
5. OAuth & OpenID Connect Single Sign On – SSO (OAuth/OIDC Client) - https://www.drupal.org/sa-contrib-2024-067
6. Print Anything - https://www.drupal.org/sa-contrib-2024-066
7. Megamenu Framework - https://www.drupal.org/sa-contrib-2024-065

Cisco Advisories and Alerts

1. Cisco NX-OS Software - https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-image-sig-bypas-pQDRQvjL

Red Hat Security Advisories

1. python3:3.6.8 - https://access.redhat.com/errata/RHSA-2024:10779
2. rhc - https://access.redhat.com/errata/RHSA-2024:10784
3. postgresql:12 - https://access.redhat.com/errata/RHSA-2024:10785
4. postgresql:15 - https://access.redhat.com/errata/RHSA-2024:10787
5. postgresql:16 - https://access.redhat.com/errata/RHSA-2024:10788

Zero Day Initiative Advisories & Updates

1. Intel - https://www.zerodayinitiative.com/advisories/ZDI-24-1641/
2. Linux Kernel - https://www.zerodayinitiative.com/advisories/ZDI-24-1642/

***** FAIR USE NOTICE*****

This message contains copyrighted material whose use has not been specifically authorized by the copyright owner. The ST-ISAC is making it available to ISAC members who have expressed a prior interest in receiving information to advance their understanding of threat activities in the interest of protecting the national infrastructure of the United States. We believe that this constitutes a 'fair use' of the copyrighted material as provided for in section 107 of the U.S. Copyright Law. If you wish to use this copyrighted material for purposes of your own that go beyond 'fair use,' you must obtain permission from the copyright owner.

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