Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

Daily Open-Source Cyber Report

December 16, 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

- NIST Issues Updated Cyber Guides Focused On Assessments And Communication
- Cisco Releases International Transportation Networking Report
- FTC Safeguards U.S. Consumers from Location Data Misuse
- Dutch People Advised To Carry Cash In Case Of Cyberattack By Russia
- Largest German Crime Marketplace Taken Down, Administrator Arrested
- Cyber Warfare 2025: The Rise of AI Weapons, Zero-Days, And State-Sponsored Chaos
- The Power Of Telematics In Traffic Management

Emerging Threats & Vulnerabilities

- Russia-Linked Apt Secret Blizzard Spotted Using Infrastructure Of Other Threat Actors
- Hackers Leveraging Cloudflare Tunnels, DNS Fast-Flux to Hide GammaDrop Malware
- SonicWall Patches 6 Vulnerabilities in Secure Access Gateway
- Solana Web3.js Library Backdoored in Supply Chain Attack
- Windows, Macos Users Targeted With Crypto-And-Info-Stealing Malware

Attacks, Breaches, & Leaks

- Ransomware Attack Cripples Wood County Computer Systems
- Geocon Data Breach
- [ELDORADO] – Ransomware Victim: Midland Turbo
- Rhode Island Residents' Data Breached in Large Cyberattack; Data May Be Leaked Soon
- 4.8 Million Healthcare Records Left Freely Accessible

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

EXECUTIVE NEWS

NIST Issues Updated Cyber Guides Focused On Assessments And Communication
Next Gov, 12/4/2024

The National Institute of Standards and Technology issued two new updates to its existing literature on gauging the efficacy of organizations' cybersecurity protocols, addressing both the selection and maintenance of a proper cybersecurity program depending on organizational needs. Released on Wednesday, the new guidance is split into two volumes looking at different stages of implementing an effective cybersecurity program. Volume 1 is focused on technical issues in information security measurement and assessment, weighing the pros and cons of qualitative assessments versus classical data analysis approaches. https://www.nextgov.com/cybersecurity/2024/12/nist-issues-updated-cyber-guides-focused-assessments-and-communication/401410/

Cisco Releases International Transportation Networking Report
ITS International, 12/11/2024

Cisco has released its 2024 State of Industrial Networking Report for Transportation, which looks at how transportation firms worldwide are designing and deploying operational technology to improve performance, compliance and cybersecurity. The free research is available exclusively at ITS International: click here to download. In partnership with Sapio Research, the Cisco report was compiled by speaking to 146 senior industry professionals at firms with annual revenues of over $100 million, in 17 countries. https://www.itsinternational.com/news/cisco-releases-international-transportation-networking-report

FTC Safeguards U.S. Consumers from Location Data Misuse
Infosecurity Magazine, 12/4/2024

The Federal Trade Commission (FTC) has banned data brokers Gravy Analytics and Mobilewalla from collecting, using or selling sensitive location data that reveals Americans' visits to places like healthcare facilities, military bases and religious institutions. The settlements, announced on Tuesday, also require both companies to delete previously collected data and impose strict controls to prevent future violations. The FTC accused Gravy Analytics, along with its subsidiary Venntel, and Mobilewalla of violating privacy laws by gathering detailed location data without consumer consent. This data was sold to third parties, including advertisers and government agencies, and used to identify visits to sensitive locations. https://www.infosecurity-magazine.com/news/ftc-safeguards-us-location-data/

Dutch People Advised To Carry Cash In Case Of Cyberattack By Russia
Data Breaches, 12/13/2024

The Dutch Central Bank has issued an unprecedented warning to the public to keep cash at home due to the risk of cyberattacks from Russia. Officials are concerned that cyberattacks have the potential to cause massive disruption to digital banking systems and want citizens to have some cash on them as an insurance policy. The Dutch Central Bank did not tell clients exactly how much money they should hide at home – but they promised more detailed instructions in the new year. On Newstalk Breakfast, Cyber Risk International CEO Paul Dwyer said the Dutch Central Bank's alert is a "stark warning". https://databreaches.net/2024/12/13/dutch-people-advised-to-carry-cash-in-case-of-cyberattack-by-russia/

Largest German Crime Marketplace Taken Down, Administrator Arrested
Security Week, 12/3/2024

Crimenetwork has been around since 2012, being used to trade various types of illegal goods and services, including stolen information, drugs and counterfeit documents. Authorities said the platform had over 100,000 buyers and 100 sellers, most of them likely from German-speaking countries. Investigators determined that nearly $100 million in Bitcoin and Monero cryptocurrencies were transferred through Crimenetwork between 2018 and 2024. Operators received a commission of 1-5% from each sale. German police arrested an alleged administrator of the platform on Monday, seizing evidence, vehicles, and cryptocurrency worth roughly €1 million. https://www.securityweek.com/largest-german-crime-marketplace-taken-down-administrator-arrested/

Cyber Warfare 2025: The Rise of AI Weapons, Zero-Days, And State-Sponsored Chaos
Beta News, 12/2/2024

As we approach 2025, the notion of warfare is increasingly shifting from the physical to the digital domain. Cyberwarfare, once considered a supplementary tool for traditional military operations, has now emerged as a primary weapon for nations seeking to assert dominance or inflict damage on their adversaries without the need for physical conflict. Simply put, it is easier, requires fewer resources, and can often cause maximum damage without sustained efforts. The rise of AI-driven cyber weapons, zero-day vulnerabilities, and state-sponsored cyberattacks is creating an unprecedented era of digital warfare. Nation-states and rogue factions are rapidly integrating cyberattacks into their military arsenals, with cyber operations becoming a first-strike option in geopolitical conflicts. https://betanews.com/2024/12/03/cyberwarfare-2025-the-rise-of-ai-weapons-zero-days-and-state-sponsored-chaos/

The Power Of Telematics In Traffic Management
TTI, 12/11/2024

Telematics may not have as many use cases as V2X, but it has become a well-established form of connected vehicle technology that is evolving to deliver operational and safety advantages for the benefit of all road users – and could lead the way for future V2X vehicle integration, as Christopher Court-Dobson discovers. While vehicle-to-everything (V2X) technology is transforming safety and traffic flows, with emergency and transit signal priority and live updates for drivers and traffic managers alike, its older, more established cousin, telematics, is working behind the scenes and now becoming more advanced, delivering valuable, actionable information for city and fleet managers.
https://www.traffictechnologytoday.com/news/connected-vehicles-infrastructure/feature-the-power-of-telematics-in-traffic-management.html

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

TECHNICAL SUMMARY

EMERGING THREATS & EXPLOITS

- ***Russia-Linked Apt Secret Blizzard Spotted Using Infrastructure Of Other Threat Actors -*** Researchers from Microsoft Threat Intelligence collected evidence that the Russia-linked ATP group Secret Blizzard (aka Turla, Snake, Uroburos, Waterbug, Venomous Bear and KRYPTON) has used the tools and infrastructure of at least 6 other threat actors during the past 7 years. https://securityaffairs.com/171699/apt/secret-blizzard-using-infrastructure-of-other-threat-actors.html
- ***Hackers Leveraging Cloudflare Tunnels, DNS Fast-Flux to Hide GammaDrop Malware*** - The threat actor known as Gamaredon has been observed leveraging Cloudflare Tunnels as a tactic to conceal its staging infrastructure hosting a malware called GammaDrop. https://thehackernews.com/2024/12/hackers-leveraging-cloudflare-tunnels.html
- ***SonicWall Patches 6 Vulnerabilities in Secure Access Gateway -*** SonicWall this week announced patches for multiple vulnerabilities in the SMA100 SSL-VPN secure access gateway, including high-severity flaws leading to remote code execution (RCE). https://www.securityweek.com/sonicwall-patches-6-vulnerabilities-in-secure-access-gateway/
- ***Windows, Macos Users Targeted With Crypto-And-Info-Stealing Malware –*** Downloading anything from the internet is a gamble these days: you might think that you are downloading an innocuous app from a legitimate firm but thanks to clever misuse of AI and some social engineering, you can end up with information and cryptocurrency-stealing malware. https://www.helpnetsecurity.com/2024/12/06/information-cryptocurrency-stealing-malware-windows-macos/

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

ATTACKS, BREACHES & LEAKS

- ***Ransomware Attack Cripples Wood County Computer Systems -*** A ransomware attack has blocked the ability of Wood County offices to access the county's servers, impacting functions at the sheriff's office, jail, common pleas court, and other county offices. https://www.toledoblade.com/local/suburbs/2024/12/10/ransomware-attack-cripples-wood-county-computer-systems/stories/20241210087
- ***Geocon Data Breach*** - Geocon provides a range of professional engineering consulting services, specializing in geotechnical engineering, materials testing, environmental consulting, and engineering geology. https://www.breachsense.com/breaches/geocon-data-breach/
- ***[ELDORADO] – Ransomware Victim: Midland Turbo -*** The ransomware leak page for Midland Turbo, a company operating in the manufacturing sector, indicates a data breach affecting their operations. Midland Turbo is based in the United Kingdom and specializes in industrial machinery and equipment, specifically turbo reconditioning. The company is noted for its relatively small size, having fewer than 25 employees and a facility of 7000 square feet. https://www.redpacketsecurity.com/eldorado-ransomware-victim-midland-turbo/
- ***Rhode Island Residents' Data Breached in Large Cyberattack; Data May Be Leaked Soon*** - The personal and private information of possibly hundreds of thousands of people who applied for government assistance in Rhode Island could be in the hands of hackers after a huge cyberattack, state officials said on Friday. https://databreaches.net/2024/12/14/personal-data-of-rhode-island-residents-breached-in-large-cyberattack/
- ***4.8 Million Healthcare Records Left Freely Accessible*** - Your main business is healthcare, so your excuse when you get hacked is that you didn't have the budget to secure your network. Am I right? So, in order to prevent a ransomware gang from infiltrating your network, you could just give them what they want—all your data. https://www.malwarebytes.com/blog/news/2024/12/4-8-million-healthcare-records-left-freely-accessible

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. Adobe - https://www.cve.org/CVERecord?id=CVE-2024-20767
2. Microsoft - https://www.cve.org/CVERecord?id=CVE-2024-35250

SUSE Security Updates

1. Libphonenumber - https://www.suse.com/support/update/announcement/2024/suse-fu-20244320-1
2. Firewalld - https://www.suse.com/support/update/announcement/2024/suse-ru-20244321-1
3. nvidia-open-driver-G06-signed - https://www.suse.com/support/update/announcement/2024/suse-ru-20244322-1
4. MozillaFirefox - https://www.suse.com/support/update/announcement/2024/suse-su-20244324-1
5. go1.22-openssl - https://www.suse.com/support/update/announcement/2024/suse-ru-20244325-1
6. python-aiohttp - https://www.suse.com/support/update/announcement/2024/suse-su-20244327-1
7. vim - https://www.suse.com/support/update/announcement/2024/suse-su-20244330-1

Gentoo Security Advisories

1. NVIDIA Drivers - https://security.gentoo.org/glsa/202412-20

Fedora Security Advisories

1. Kernel - https://lwn.net/Articles/1002299
2. Bpftool - https://lwn.net/Articles/1002294
3. golang-x-crypto - https://lwn.net/Articles/1002298

Debian Security Advisories

1. gst-plugins-base1.0 - https://lists.debian.org/debian-security-announce/2024/msg00247.html

Check Point Security Advisories

1. Ivanti - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2021-2111.html

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

Red Hat Security Advisories

1. python3.11 - https://access.redhat.com/errata/RHSA-2024:11111
2. gstreamer1-plugins-base - https://access.redhat.com/errata/RHSA-2024:11117

Ubuntu Security Notices

1. Mpmath - https://ubuntu.com/security/notices/USN-7160-1
2. Curl - https://ubuntu.com/security/notices/USN-7162-1
3. Docker - https://ubuntu.com/security/notices/USN-7161-1
4. Linux Kernel - https://ubuntu.com/security/notices/USN-7163-1