Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

Daily Open-Source Cyber Report

November 14, 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

The Current Threat Environment

Critical infrastructure faces a wide range of threats and risks, from naturally occurring events to human induced disruptions of both accidental and malicious origins. Numerous natural hazards adversely affect physical critical infrastructure such as transportation networks, telecommunications systems, and energy infrastructure. The threat of terrorism and targeted violence remains elevated and is increasingly local and often aimed at public gatherings and populated spaces. The diversity, complexity, and expanse of our nation's physical infrastructure pose their own unique challenges. Additionally, critical infrastructure assets and systems are highly interconnected and interdependent, both domestically and internationally, increasing the likelihood of cascading failures across multiple sectors. Increased digitization of the systems and processes that underpin the functioning of critical infrastructure amplifies the risk for assets and systems' exposure to heightened physical and cyber threats from malicious actors. The impact of cyberattacks is costly in nature, as governments and critical infrastructure owners and operators spend millions of dollars rectifying the damage caused to their assets, systems, and reputations. A shifting geopolitical landscape intensified national security concerns and demonstrated that targeting critical infrastructure can be a primary attack vector. This can occur both in a conflict setting, as well as through indirect, long-term foreign interference campaigns. These concerns highlight that domestic investment in infrastructure security and resilience can both strengthen national security and serve as a strategic deterrent. All of these factors demand a greater focus on resilience. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/criticalinfrastructure-security-and-resilience-month

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

AT-A-GLANCE

Executive News

- Researchers Develop Ai Tool To Safeguard Vehicles From Cyber Threats
- Cyber Attack on UK Train Station WiFi Sparks Safety Concerns
- Unwrapping The Emerging Interlock Ransomware Attack
- Defenders Outpace Attackers in AI Adoption
- Barcelona Tramway Deploys Alstom Aps Catenary-Free Tech
- 5 Most Common Malware Techniques in 2024
- How Early-Stage Companies Can Go Beyond Cybersecurity Basics

Emerging Threats & Vulnerabilities

- Hackers Can Access Mazda Vehicle Controls Via System Vulnerabilities
- Malicious Python Package Typosquats Popular 'fabric' SSH Library, Exfiltrates AWS Credentials
- Critical Bug In Cisco UWRB Access Points Allows Attackers To Run Commands As Root
- VEILDrive Attack Exploits Microsoft Services to Evade Detection and Distribute Malware
- GoZone Ransomware Accuses And Threatens Victims

Attacks, Breaches, & Leaks

- Followmont Transport Confirms ‘Unauthorized Access To Our Systems’
- Texas Oilfield Supplier Newpark Resources Suffered A Ransomware Attack
- Ransomware Attack Hits Mount Laurel Utilities by Qilin Group
- Form I-9 Compliance Data Breach Impacts Over 190,000 People
- Investigation Underway After Alberta Crown Corporation Hit By Cyberattack

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

EXECUTIVE NEWS

Researchers Develop Ai Tool To Safeguard Vehicles From Cyber Threats
Eurek Alert!, 11/11/2024

How to preserve the privacy of the so-called Internet of Vehicles (IoV) has emerged as a major challenge due to geographical mobility of vehicles and insufficient resources, the scientists say. The problem has aggravated, according to the scientists, due to the "limited resources of onboard units (OBUs)" and the shortcomings of embedded sensors installed in vehicles, which "lure the adversaries to launch various types of attacks." "Thus, lightweight but reliable authentication schemes need to be designed to combat these attacks," they write in the IEEE Internet of Things Journal. The research is co-authored by scientists from the University of Sharjah in the United Arab Emirates, the University of Maryland in the US, and Abdul Wali Khan University Mardan, Pakistan. https://www.eurekalert.org/news-releases/1064387

Cyber Attack on UK Train Station WiFi Sparks Safety Concerns
electropages, 11/12/2024

The recent cyber attack on UK train stations via public WiFi networks has raised concerns about cybersecurity and public safety. As authorities work to investigate and prevent such incidents, the incident prompts questions about the motives behind the attack, the vulnerabilities in public WiFi networks that were exploited, and the potential impact on public trust in using such services. How can cybersecurity measures be strengthened to safeguard public infrastructure from similar attacks in the future, what steps are being taken to identify and prosecute those responsible for this cyber attack, and how might this incident influence the public's perception of using public WiFi networks in public spaces?
https://www.electropages.com/blog/2024/11/train-station-wifi-attacked-across-uk-dangers-public-wifi

Unwrapping The Emerging Interlock Ransomware Attack
Cisco Talos Blog, 11/12/2024

Interlock first appeared in public reporting in September 2024 and has been observed launching big-game hunting and double extortion attacks. The group has notably targeted businesses in a wide range of sectors, which at the time of reporting includes healthcare, technology, government in the U.S. and manufacturing in Europe, according to the data leak site disclosure, indicating their targeting is opportunistic. Like other ransomware players in the big-game hunting space, Interlock also operates a data leak site called "Worldwide Secrets Blog," providing links to victims' leaked data, chat support for victims' communications, and the email address, "interlock@2mail[.]co".
https://blog.talosintelligence.com/emerging-interlock-ransomware/

Defenders Outpace Attackers in AI Adoption
Infosecurity Magazine, 11/6/2024

Cybercriminals' use of AI is more limited than is generally reported or demonstrated by security researchers. Meanwhile, investment in AI by the cybersecurity sector is set to give defenders the edge over threat actors, according to Trend Micro's Director, Forward Looking Threat Research - Cybercrime Research, Robert McArdle. Speaking during IRISSCON 2024 in Dublin, McArdle said that given the contrasting scale of investment and emphasis on AI in cybersecurity, defenders will gain an advantage over attackers. https://www.infosecurity-magazine.com/news/defenders-attackers-ai-adoption/

Barcelona Tramway Deploys Alstom Aps Catenary-Free Tech
Railway Technology, 11/7/2024

Barcelona's tramway has made the first Spanish deployment of Alstom's APS catenary-free technology, enhancing the city's sustainable transport infrastructure. The technology was installed on a new 2km extension, expected to carry an additional 24,000 passengers daily. This development aligns with Barcelona's broader strategy for eco-friendly, accessible, and equitable urban development. The Barcelona Metropolitan Transport Authority (ATM) has launched the commercial service of this extension, utilising Alstom's APS system. https://upstream.auto/blog/cybersecurity-risks-in-fleet-telematics/

5 Most Common Malware Techniques in 2024
The Hacker News, 11/7/2024

Tactics, techniques, and procedures (TTPs) form the foundation of modern defense strategies. Unlike indicators of compromise (IOCs), TTPs are more stable, making them a reliable way to identify specific cyber threats. Here are some of the most commonly used techniques, according to ANY.RUN's Q3 2024 report on malware trends, complete with real-world examples. Disrupting Windows Event Logging helps attackers prevent the system from recording crucial information about their malicious actions. Without event logs, important details such as login attempts, file modifications, and system changes go unrecorded, leaving security solutions and analysts with incomplete or missing data.
https://thehackernews.com/2024/11/5-most-common-malware-techniques-in-2024.html

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

How Early-Stage Companies Can Go Beyond Cybersecurity Basics
Cyber Scoop, 11/6/2024

The digital landscape has become a battleground, with cybercriminals constantly evolving their tactics and outmaneuvering even the most advanced defenses. Phishing scams are becoming increasingly sophisticated, zero-day vulnerabilities are emerging at an alarming rate, and ransomware attacks are crippling organizations worldwide. To stay ahead of this ever-shifting threat landscape, businesses must adopt a proactive approach to cybersecurity that goes beyond mere compliance. It's no surprise that the threat landscape is more bold and complex than ever before. Hackers are constantly refining their tactics, exploiting new vulnerabilities, and finding ways to bypass even the most sophisticated security measures. https://cyberscoop.com/cybersecurity-for-startups-early-stage-companies/

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

TECHNICAL SUMMARY

EMERGING THREATS & EXPLOITS

- ***Hackers Can Access Mazda Vehicle Controls Via System Vulnerabilities*** - Cybersecurity researchers at ZDI (Zero Day Initiative) have identified several critical vulnerabilities in Mazda's infotainment systems, specifically in the Connectivity Master Unit (CMU) installed in multiple Mazda car models, including the Mazda 3 from the years 2014 to 2021. https://hackread.com/hackers-mazda-vehicle-controls-system-vulnerabilities/
- ***Malicious Python Package Typosquats Popular 'fabric' SSH Library, Exfiltrates AWS Credentials*** - The Socket Research Team has discovered a malicious Python package, fabrice, that is typosquatting the popular fabric SSH automation library. The threat of malware delivered through typosquatted libraries remains a significant and growing risk to developers using open source software, as demonstrated by the massive malware campaign that recently hit npm. https://socket.dev/blog/malicious-python-package-typosquats-fabric-ssh-library
- ***Critical Bug In Cisco UWRB Access Points Allows Attackers To Run Commands As Root -*** "This vulnerability is due to improper validation of input to the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system of the affected device." https://securityaffairs.com/170646/security/cisco-uwrb-cririca l-flaw.html
- ***VEILDrive Attack Exploits Microsoft Services to Evade Detection and Distribute Malware –*** An ongoing threat campaign dubbed VEILDrive has been observed taking advantage of legitimate services from Microsoft, including Teams, SharePoint, Quick Assist, and OneDrive, as part of its modus operandi. https://thehackernews.com/2024/11/veildrive-attack-exploits-microsoft.html
- ***Gozone Ransomware Accuses And Threatens Victims -*** A new ransomware dubbed GoZone is being leveraged by attackers that don't seem to be very greedy: they are asking the victims to pay just $1,000 in Bitcoin if they want their files decrypted. https://www.helpnetsecurity.com/2024/11/06/gozone-ransomware-d3pru/

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

ATTACKS, BREACHES & LEAKS

- ***Followmont Transport Confirms 'Unauthorised Access To Our Systems'*** – The Akira ransomware gang has claimed Queensland-headquartered transport company Followmont Transport as a victim on its darknet leak site overnight. https://www.cyberdaily.au/security/11340-exclusive-followmont-transport-confirms-unauthorised-access-to-our-systems
- ***Texas Oilfield Supplier Newpark Resources Suffered A Ransomware Attack*** - The company immediately activated its cybersecurity response plan and launched an investigation into the incident with the help of external experts. https://securityaffairs.com/170696/cyber-crime/newpark-resources-ransomware-attack.html
- ***Ransomware Attack Hits Mount Laurel Utilities by Qilin Group*** - The Mount Laurel Municipal Utilities Authority (MLTMUA), a key provider of water and wastewater services to approximately 18,000 residents in Mount Laurel Township, New Jersey, has been targeted by the notorious Qilin ransomware group. This attack, discovered on November 4, highlights the vulnerabilities of essential service providers to sophisticated cyber threats. https://ransomwareattacks.halcyon.ai/attacks/ransomware-attack-hits-mount-laurel-utilities-by-qilin-group
- ***Form I-9 Compliance Data Breach Impacts Over 190,000 People*** - In late May, the company started informing customers that someone had gained unauthorized access to its network in early February. The intrusion was detected on April 12 and some systems were shut down as part of the company's incident response process. https://www.securityweek.com/form-i-9-compliance-data-breach-impacts-over-190000-people/
- ***Investigation Underway After Alberta Crown Corporation Hit By Cyberattack*** - An Alberta Crown corporation says it recently experienced "network issues" after it was the target of a cyberattack. Dwayne Brunner, a spokesman for Alberta Innovates, wouldn't confirm when the issues began, but said an investigation is underway and all network problems have been resolved. https://www.thestar.com/news/canada/alberta/investigation-underway-after-alberta-crown-corporation-hit-by-cyberattack/article_3dd179d9-61ef-57f7-b462-b6ab48c15a20.html

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. Siemens –
    a. https://www.cisa.gov/news-events/ics-advisories/icsa-24-319-01
    b. https://www.cisa.gov/news-events/ics-advisories/icsa-24-319-02
    c. https://www.cisa.gov/news-events/ics-advisories/icsa-24-319-03
    d. https://www.cisa.gov/news-events/ics-advisories/icsa-24-319-04
    e. https://www.cisa.gov/news-events/ics-advisories/icsa-24-319-05
    f. https://www.cisa.gov/news-events/ics-advisories/icsa-24-319-06
    g. https://www.cisa.gov/news-events/ics-advisories/icsa-24-319-07
    h. https://www.cisa.gov/news-events/ics-advisories/icsa-24-319-08
    i. https://www.cisa.gov/news-events/ics-advisories/icsa-24-319-09
    j. https://www.cisa.gov/news-events/ics-advisories/icsa-24-319-10
    k. https://www.cisa.gov/news-events/ics-advisories/icsa-24-319-11
    l. https://www.cisa.gov/news-events/ics-advisories/icsa-24-319-12
2. Rockwell –
    a. https://www.cisa.gov/news-events/ics-advisories/icsa-24-319-13
    b. https://www.cisa.gov/news-events/ics-advisories/icsa-24-319-14
    c. https://www.cisa.gov/news-events/ics-advisories/icsa-24-319-15
3. Hitachi Energy - https://www.cisa.gov/news-events/ics-advisories/icsa-24-319-16
4. 2N Access Commander - https://www.cisa.gov/news-events/ics-advisories/icsa-24-319-17
5. Elvaco M-Bus Metering Gateway - https://www.cisa.gov/news-events/ics-advisories/icsa-24-291-01
6. Baxter Life2000 Ventilation System - https://www.cisa.gov/news-events/ics-medical-advisories/icsma-24-319-01

SUSE Security Updates

1. Buildah - https://www.suse.com/support/update/announcement/2024/suse-su-20243988-1
2. nodejs16 - https://www.suse.com/support/update/announcement/2024/suse-ru-20243990-1

Fedora Security Advisories

1. xorg-x11-server-Xwayland - https://lwn.net/Articles/998123
2. mingw-expat - https://lwn.net/Articles/998118
3. webkit2gtk4.0 –
    a. https://lwn.net/Articles/998121
    b. https://lwn.net/Articles/998121

4. python3.6 - https://lwn.net/Articles/998120
5. llama-cpp - https://lwn.net/Articles/998117

Red Hat Security Advisories

1. tigervnc - https://access.redhat.com/errata/RHSA-2024:9690
2. binutils - https://access.redhat.com/errata/RHSA-2024:9689
3. webkit2gtk3 –
    a. https://access.redhat.com/errata/RHSA-2024:9680
    b. https://access.redhat.com/errata/RHSA-2024:9679
4. Squid - https://access.redhat.com/errata/RHSA-2024:9677

Ubuntu Security Notices

1. PHP - https://ubuntu.com/security/notices/USN-7049-2
2. Linux Kernel - https://ubuntu.com/security/notices/USN-7110-1
3. Go - https://ubuntu.com/security/notices/USN-7109-1

Oracle Linux Security Update

1. Libsoup - https://lwn.net/Articles/998136
2. Tigervnc - https://lwn.net/Articles/998138