Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

Daily Open-Source Cyber Report

November 5, 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

Security and Resiliency Guide: Counter-Improvised Explosive Device (C-IED) Concepts, Common Goals, and Available Assistance

The Security and Resiliency Guide: Counter-IED Concepts, Common Goals, and Available Assistance (SRG C-IED) is intended to help communities, individual organizations, and facility owner/operators plan and implement C-IED activities within their overall public safety and emergency management approach. You can use it to understand the IED risk landscape in the U.S. and your locale; apply common IED-specific security and resiliency goals; and leverage available U.S. Government resources to build and sustain preparedness. The SRG C-IED was created by the Department of Homeland Security in coordination with the Federal Bureau of Investigation, with contributions from IED and C-IED experts and stakeholders. https://www.cisa.gov/publication/security-and-resiliency-guide-and-annexes

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

AT-A-GLANCE

Executive News

- U.S. Government Issues New TLP Guidance for Cross-Sector Threat Intelligence Sharing
- FMCSA To Use Identity Verification To Combat Fraud In Trucking
- AI-Powered BEC Scams Zero in on Manufacturers
- Navigating the Cybersecurity Landscape in Logistics: Risks, Solutions, And Opportunities
- Fraudsters Revive Old Tactics Mixed With Modern Technology
- Put End-of-Life Software to Rest
- Why AI is a Gamechanger for Fleet Safety

Emerging Threats & Vulnerabilities

- Crooks Bank On Microsoft's Search Engine To Phish Customers
- Recent Version of LightSpy iOS Malware Packs Destructive Capabilities
- QNAP Fixes Nas Backup Software Zero-Day Exploited At Pwn2own
- Researchers Uncover Vulnerabilities in Open-Source AI and ML Models
- New Type of Job Scam Targets Financially Vulnerable Populations

Attacks, Breaches, & Leaks

- Telematics Giant Microlise Suffers Cyber Attack
- City Of Columbus Breach Affects Around Half A Million Citizens
- Colorado Accidentally Put Voting System Passwords Online, but Officials Say Election Is Secure
- Hackers Steal 15,000 Cloud Credentials From Exposed Git Config Files
- Macron's Bodyguards Reveal His Location By Sharing Strava Data

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

EXECUTIVE NEWS

U.S. Government Issues New TLP Guidance for Cross-Sector Threat Intelligence Sharing
The Hacker News, 10/29/2024

The U.S. government (USG) has issued new guidance governing the use of the Traffic Light Protocol (TLP) to handle threat intelligence information shared between the private sector, individual researchers, and Federal Departments and Agencies. "The USG follows TLP markings on cybersecurity information voluntarily shared by an individual, company, or other any organization, when not in conflict with existing law or policy," it said. "We adhere to these markings because trust in data handling is a key component of collaboration with our partners." In using these designations, the idea is to foster trust and collaboration in the cybersecurity community while ensuring that the information is shared in a controlled manner, the government added. https://thehackernews.com/2024/10/us-government-issues-new-tlp-guidance.html

FMCSA To Use Identity Verification To Combat Fraud In Trucking
Landline Media, 11/4/2024

Identity verification is one of the ways the Federal Motor Carrier Safety Administration hopes to combat fraud in the trucking industry. As part of FMCSA's efforts to modernize its registration system, new carriers are expected to be required to confirm their identity before the year is over. Existing carriers will likely need to go through the verification process sometime in 2025. "It's kind of a QR code that you will scan or go online via your laptop or smartphone," said Jay Grimes, OOIDA's director of federal affairs. "It takes facial recognition and confirms your individual identity … Hopefully this will create another layer of fraud prevention. (Fraud) has run rampant throughout the industry." https://landline.media/fmcsa-to-use-identity-verification-to-combat-fraud-in-trucking/

AI-Powered BEC Scams Zero in on Manufacturers
Infosecurity Magazine, 10/28/2024

Business email compromise (BEC) threats are on the rise and now account for over half of all phishing attempts, with manufacturers particularly badly hit, according to Vipre Security Group. The security vendor used proprietary intelligence to compile its Email Threat Trends Report: Q3 2024, published this morning. It revealed that around 12% of the 1.8 billion emails that Vipre processed globally in the period were classified as malicious, with BEC accounting for 58% of phishing attempts. In fact, BEC is often described as "pretexting" – a more complex form of phishing in which the threat actor crafts an elaborate back story to gain the victim's trust. https://www.infosecurity-magazine.com/news/aipowered-bec-scams-manufacturers/

Navigating the Cybersecurity Landscape in Logistics: Risks, Solutions, And Opportunities
Global Trade Magazine, 11/1/2024

With the rising globalization, global trade could reach almost USD 32 trillion by the end of year 2024. The mushrooming international trade instilling the requirement for cross border transport along with the logistics services has increased. However, the logistic supply chains have become lucrative target for the malicious cyber attackers. It has been estimated that 27 incidents affected transportation and logistics companies between July 1, 2023, and July 30, 2024. As logistics and supply chains become increasingly digital, the need for robust cybersecurity has never been more essential. From the tracking and transportation of goods to inventory management and final delivery, every step in the logistics industry relies heavily on digital systems. https://www.globaltrademag.com/navigating-the-cybersecurity-landscape-in-logistics-risks-solutions-and-opportunities/

Fraudsters Revive Old Tactics Mixed With Modern Technology
Help Net Security, 11/1/2024

Scammers are going back to basics with an increase of physical theft over the past six months, capitalizing on the window between the theft and the victim's awareness. After a theft, the most common ways the criminals are capitalizing on their theft by purchasing gift cards or physical goods to resell, or even using the card number online for money transfers. Similarly, in March of 2023, Visa identified an emerging threat dubbed "digital pickpocketing," where cybercriminals use a mobile point-of-sale device to tap against unsuspecting consumers' wallets and initiate a payment, often in crowded areas. Consumers are falling victim to scams where fraudsters pose as representatives from the government, including agencies like the USPS, the FBI and the IRS. In the first three months of 2024, the average government impersonation scam victim in the US lost $14,000 in cash, totaling more than $20 million. https://www.helpnetsecurity.com/2024/10/28/payments-fraud-schemes/

Put End-of-Life Software to Rest
Dark Reading, 10/28/2024

When you've bought a haunted house, the worst thing you can do is decide to just live with it. Yet in every horror movie, there's always that one person — usually the father — who doesn't want to leave. Plates are flying off the shelves, blood is erupting from the sink, and Dad is ignoring all of it while pruning the ficus in the living room. Dad doesn't last long in those movies, and it's because he's ignoring one universal truth: Denying that a threat is real won't protect you from it. You'd think security-minded organizations would have learned that lesson by now. Unfortunately, many are just like Dad, resigned to an IT infrastructure that's lousy with ghosts. https://www.darkreading.com/vulnerabilities-threats/put-end-life-software-rest

Why AI is a Gamechanger for Fleet Safety
Supply Chain Digital, 11/4/2024

New research from video telematics firm Netradyne, shared at the Gartner Supply Chain Planning Summit, highlights a rising trend: AI could be a game-changer in fleet safety for logistics and transportation. Presently, only 33% of professionals in the field are using AI to enhance fleet safety, but 81% intend to integrate AI-based solutions within the next year. This shift is expected to drive down risks and improve operational accuracy, helping companies improve fleet safety, reduce incidents and save on costs. Netradyne, known for its AI-driven fleet management solution, Driver•i, is a leader in this technological shift. https://supplychaindigital.com/technology/Netradyne-why-ai-is-a-gamechanger-for-fleet-safety

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

TECHNICAL SUMMARY

EMERGING THREATS & EXPLOITS

- ***Crooks Bank On Microsoft's Search Engine To Phish Customers -*** We identified a new wave of phishing for banking credentials that targets consumers via Microsoft's search engine. A Bing search query for 'Keybank login' currently returns malicious links on the first page, and sometimes as the top search result. We have reported the fraudulent sites to Microsoft already. https://www.malwarebytes.com/blog/scams/2024/11/crooks-bank-on-microsofts-search-engine-to-phish-customers
- ***Recent Version of LightSpy iOS Malware Packs Destructive Capabilities -*** A recent iOS-targeting version of the LightSpy malware includes over a dozen new plugins, many with destructive capabilities, according to cybersecurity firm ThreatFabric. https://www.securityweek.com/recent-version-of-lightspy-ios-malware-packs-destructive-capabilities/
- ***QNAP Fixes Nas Backup Software Zero-Day Exploited At Pwn2own*** - QNAP has fixed a critical zero-day vulnerability exploited by security researchers on Thursday to hack a TS-464 NAS device during the Pwn2Own Ireland 2024 competition. https://www.bleepingcomputer.com/news/security/qnap-fixes-nas-backup-software-zero-day-exploited-at-pwn2own/
- ***Researchers Uncover Vulnerabilities in Open-Source AI and ML Models*** - A little over three dozen security vulnerabilities have been disclosed in various open-source artificial intelligence (AI) and machine learning (ML) models, some of which could lead to remote code execution and information theft. https://thehackernews.com/2024/10/researchers-uncover-vulnerabilities-in.html
- ***New Type of Job Scam Targets Financially Vulnerable Populations*** -A surge in online job scams targeting financially vulnerable individuals has been identified by cybersecurity experts at Proofpoint. Known as "job scamming," this new tactic mirrors the existing "pig butchering" fraud model but aims at a broader audience by preying on job seekers looking for remote, flexible work. https://www.infosecurity-magazine.com/news/job-scam-targets-financially/

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

ATTACKS, BREACHES & LEAKS

- ***Telematics Giant Microlise Suffers Cyber Attack*** –Microlise has suffered a cyber attack, with a large proportion of the company's services affected, leaving fleets without some tracking services. The Microlise board says it has appointed external cyber security specialists whose investigations are underway to establish the nature and extent of the incident. https://www.fleetnews.co.uk/news/telematics-giant-microlise-suffers-cyber-attack
- ***City Of Columbus Breach Affects Around Half A Million Citizens*** - A ransomware attack against the City of Columbus, Ohio—which drew public scrutiny following the city government's attempt to silence a researcher who told the public about the attack—has received a little more detail from an unexpected source: The Attorney General for the state of Maine. https://www.malwarebytes.com/blog/news/2024/11/city-of-columbus-breach-affects-around-half-a-million-citizens
- ***Colorado Accidentally Put Voting System Passwords Online, but Officials Say Election Is Secure*** - Voting system passwords were mistakenly put on the Colorado Secretary of State's website for several months before being spotted and taken down, but the lapse did not pose an immediate threat to the upcoming election, said state election officials Tuesday. https://www.securityweek.com/colorado-accidentally-put-voting-system-passwords-online-but-officials-say-election-is-secure/
- ***Hackers Steal 15,000 Cloud Credentials From Exposed Git Config Files*** - A large-scale malicious operation named "EmeraldWhale" scanned for exposed Git configuration files to steal over 15,000 cloud account credentials from thousands of private repositories. https://www.bleepingcomputer.com/news/security/hackers-steal-15-000-cloud-credentials-from-exposed-git-config-files/
- ***Macron's Bodyguards Reveal His Location By Sharing Strava Data*** - The French equivalent of the US Secret Service may have been letting their guard down, as an investigation showed they are easily trackable via the fitness app Strava. https://www.theregister.com/2024/10/29/macron_location_strava/

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

SECURITY VULNERABILITIES, ALERTS, ADVISORIES, & UPDATES

SUSE Security Updates

1. govulncheck-vulndb - https://www.suse.com/support/update/announcement/2024/suse-su-20243911-1
2. openssl-ibmca - https://www.suse.com/support/update/announcement/2024/suse-ru-20243912-1
3. buildah - https://www.suse.com/support/update/announcement/2024/suse-ru-20243913-1
4. protobuf - https://www.suse.com/support/update/announcement/2024/suse-ru-20243914-1
5. grpc - https://www.suse.com/support/update/announcement/2024/suse-ou-20240801-2

Fedora Security Advisories

1. python-quart - https://lwn.net/Articles/997011
2. llama-cpp - https://lwn.net/Articles/997010

Mageia Security Advisories

1. digicam - http://advisories.mageia.org/MGAA-2024-0223.html
2. grub2 - http://advisories.mageia.org/src_grub2.html

Check Point Security Advisories

1. Linux kernel - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2023-1922.html
2. PTZOptics - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-1042.html
3. Wordpress –
    a. https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2018-2852.html
    b. https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2022-2138.html
    c. https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2020-4207.html
4. TInyproxy - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2023-1693.html
5. Dolibarr - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2022-1599.html
6. CyberPanel - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-1036.html
7. Kemp - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-1010.html

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

Red Hat Security Advisories

1. OCP Tools 4.15 Openshift Jenkins –
    a. https://access.redhat.com/errata/RHSA-2024:8884
    b. https://access.redhat.com/errata/RHSA-2024:8885
    c. https://access.redhat.com/errata/RHSA-2024:8886
    d. https://access.redhat.com/errata/RHSA-2024:8887
2. Satellite 6.16.0 - https://access.redhat.com/errata/RHSA-2024:8906

Ubuntu Security Notices

1. OpenJPEG - https://ubuntu.com/security/notices/USN-7083-1
2. Ruby - https://ubuntu.com/security/notices/USN-7091-1
3. mpg123 - https://ubuntu.com/security/notices/USN-7092-1

Oracle Linux Security Update

1. firefox - https://lwn.net/Articles/997014
2. openexr - https://lwn.net/Articles/997015
3. xorg-x11-server and xorg-x11-server-Xwayland - https://lwn.net/Articles/997018
4. thunderbird –
    a. https://lwn.net/Articles/997016
    b. https://lwn.net/Articles/997017

Other

1. Scapy Packet Manipulation Tool 2.6.1 - https://packetstormsecurity.com/files/download/182514/scapy-2.6.1.tar.gz
2. Chrome Dev for Desktop - https://chromereleases.googleblog.com/2024/11/chrome-dev-for-desktop-update.html