Information Sharing &
Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

# Daily Open-Source Cyber Report

December 23, 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 Releases Best Practice Guidance for Mobile Communications
- Iranian Hackers Use IOCONTROL Malware to Target OT, IoT Devices in US, Israel
- Notorious Nigerian cybercriminal tied to BEC scams extradited to U.S.
- Borderlands Mexico: Cyberattacks rise in Mexico as cross-border trade grows
- Top 8 Automotive Manufacturing Trends Shaping the Future of 2025
- How Cryptocurrency Turns to Cash in Russian Banks
- Managing Threats When Most of the Security Team Is Out of the Office

**Emerging Threats & Vulnerabilities**

- Hunk Companion WordPress plugin exploited to install vulnerable plugins
- Remcos RAT Malware Evolves with New Techniques
- IoT Cloud Cracked by 'Open Sesame' Over-the-Air Attack
- Researchers Uncover Symlink Exploit Allowing TCC Bypass in iOS and macOS
- Multiple flaws in Volkswagen Group’s infotainment unit allow for vehicle compromise

**Attacks, Breaches, & Leaks**

- Technical Problems Disrupt De Lijn Services: Cyber Attack Suspected
- Over 300K Prometheus Instances Exposed: Credentials and API Keys Leaking Online
- Beyondtrust Says Hackers Breached Remote Support Saas Instances
- Abrasive Supply Data Breach

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

## EXECUTIVE NEWS

**CISA Releases Best Practice Guidance for Mobile Communications**
*CISA, 12/18/2024*

Today, CISA released Mobile Communications Best Practice Guidance. The guidance was crafted in response to identified cyber espionage activity by People's Republic of China (PRC) government-affiliated threat actors targeting commercial telecommunications infrastructure, specifically addressing "highly targeted" individuals who are in senior government or senior political positions and likely to possess information of interest to these threat actors. Highly targeted individuals should assume that all communications between mobile devices—including government and personal devices—and internet services are at risk of interception or manipulation. https://www.cisa.gov/news-events/alerts/2024/12/18/cisa-releases-best-practice-guidance-mobile-communications

**Iranian Hackers Use IOCONTROL Malware to Target OT, IoT Devices in US, Israel**
*Security Week, 12/13/2024*

The malware, named IOCONTROL, has been tied by Claroty researchers to CyberAv3ngers, which claims to be a hacktivist group, but which the US government and others have linked to Iran's Islamic Revolutionary Guard Corps (IRGC). CyberAv3ngers has targeted industrial control systems (ICS) at water facilities in Ireland and the United States, including a water utility in Pennsylvania. In the Ireland attack, the hackers' actions caused serious disruptions that led to the water supply being cut off for two days. The attacks did not involve sophisticated hacking and instead relied on the fact that many organizations leave ICS exposed to the internet and protected with default credentials that can be easily obtained. https://www.securityweek.com/iranian-hackers-use-iocontrol-malware-to-target-ot-iot-devices-in-us-israel/

**Notorious Nigerian cybercriminal tied to BEC scams extradited to U.S.**
*Cyber Scoop, 12/12/2024*

Abiola Kayode, a 37-year-old Nigerian national, has been extradited from Ghana to the United States to face charges of conspiracy to commit wire fraud. Kayode, who was on the FBI's Most Wanted cybercriminal list, is charged with participating in a business email compromise (BEC) scheme and romance fraud from January 2015 to September 2016, defrauding businesses of over $6 million. The scheme involved Kayode's co-conspirators impersonating high-level executives and directing company employees to make fraudulent wire transfers. The funds were then diverted to accounts controlled by Kayode and others, many of which belonged to victims of romance scams. https://cyberscoop.com/abiola-kayode-nigerian-cybercriminal-bec-scam-extradited/

**Borderlands Mexico: Cyberattacks rise in Mexico as cross-border trade grows**
*Freight Waves, 12/15/2024*

Mexico has seen a surge in cybercrime, including ransomware, phishing, spoofing and extortion, according to the 2024 report from the LatAm Cyber Summit, and the country's trade industry is a popular target. Mexico averages about 298 malware attack attempts per minute, second only to Brazil (1,554 attack attempts per minute) in Latin America, the report said. The third annual LatAm Cyber Summit took place Nov. 26-27, in Sao Paulo. It examined how organizations can protect themselves against cyberthreats using advanced tools, employee training and national strategies. https://www.freightwaves.com/news/borderlands-mexico-cyberattacks-rise-in-mexico-as-cross-border-trade-grows

**Top 8 Automotive Manufacturing Trends Shaping the Future of 2025**
*Bleeping Computer, 12/10/2024*

The automotive manufacturing industry is evolving rapidly as manufacturers respond to technological advancements, consumer preferences, and regulatory changes. As we look ahead to 2025, these trends highlight the challenges and opportunities that manufacturers face. We explore eight most influential trends expected to define the automotive manufacturing landscape, offering insights into what lies ahead for the industry. The push toward electrification is reshaping the automotive manufacturing landscape. By 2025, we will see increased investments in EV production as automakers cater to evolving consumer demands and regulatory pressures. https://manufacturing-today.com/news/top-8-automotive-manufacturing-trends-shaping-the-future-of-2025/

**How Cryptocurrency Turns to Cash in Russian Banks**
*Kerbson Security, 12/11/2024*

A financial firm registered in Canada has emerged as the payment processor for dozens of Russian cryptocurrency exchanges and websites hawking cybercrime services aimed at Russian-speaking customers, new research finds. Meanwhile, an investigation into the Vancouver street address used by this company shows it is home to dozens of foreign currency dealers, money transfer businesses, and cryptocurrency exchanges — none of which are physically located there. Richard Sanders is a blockchain analyst and investigator who advises the law enforcement and intelligence community. Sanders spent most of 2023 in Ukraine, traveling with Ukrainian soldiers while mapping the shifting landscape of Russian crypto exchanges that are laundering money for narcotics networks operating in the region. https://krebsonsecurity.com/2024/12/how-cryptocurrency-turns-to-cash-in-russian-banks/

**Managing Threats When Most of the Security Team Is Out of the Office**
*Dark Reading, 12/20/2024*

Attackers can infiltrate corporate chat systems like Slack or Microsoft Teams and just ... watch. For months, they monitor conversations, learn who the experienced staff are, and take notes on upcoming vacation plans and each team member's communication style. Then when the company shifts to a skeleton crew — perhaps during a major holiday or summer break — they strike. For one organization, this silent reconnaissance had devastating results, says Ed Skoudis, president of the SANS Institute and founder of Counter Hack. An attacker posed as a trusted colleague in a chat channel and tricked a junior employee into making critical configuration changes while many team members were on vacation.
https://www.darkreading.com/cybersecurity-operations/managing-threats-when-security-on-vacation

# TECHNICAL SUMMARY

## EMERGING THREATS & EXPLOITS

- ***Hunk Companion Wordpress Plugin Exploited To Install Vulnerable Plugins-*** Hackers are exploiting a critical vulnerability in the "Hunk Companion" plugin to install and activate other plugins with exploitable flaws directly from the WordPress.org repository. https://www.bleepingcomputer.com/news/security/hunk-companion-wordpress-plugin-exploited-to-install-vulnerable-plugins/
- ***Remcos RAT Malware Evolves with New Techniques*** - The malware, delivered through phishing emails and malicious attachments, enables attackers to control victim machines remotely, steal data and carry out espionage. https://www.infosecurity-magazine.com/news/remcos-rat-malware-evolves-new/
- ***IoT Cloud Cracked by 'Open Sesame' Over-the-Air Attack -*** Internet of Things (IoT) vendor Ruijie Networks has shored up its Reyee cloud management platform against 10 newly discovered vulnerabilities that could have given adversaries control of thousands of connected devices in a single cyberattack. https://www.darkreading.com/ics-ot-security/iot-cloud-cracked-open-sesame-attack
- ***Researchers Uncover Symlink Exploit Allowing TCC Bypass in iOS and macOS –*** Details have emerged about a now-patched security vulnerability in Apple's iOS and macOS that, if successfully exploited, could sidestep the Transparency, Consent, and Control (TCC) framework and result in unauthorized access to sensitive information. https://thehackernews.com/2024/12/researchers-uncover-symlink-exploit.html
- ***Multiple Flaws In Volkswagen Group's Infotainment Unit Allow For Vehicle Compromise –*** A team of security researchers from cybersecurity firm PCAutomotive discovered multiple vulnerabilities in the infotainment units used in some vehicles of the Volkswagen Group. Remote attackers can exploit the flaws to achieve certain controls and track the location of cars in real time. https://securityaffairs.com/172024/hacking/volkswagen-group-infotainment-unit-flaws.html

## ATTACKS, BREACHES & LEAKS

- ***Technical Problems Disrupt De Lijn Services: Cyber Attack Suspected -*** Technical issues at De Lijn, the public transport operator in Belgium, have caused technical issues in real-time passenger information on its buses and trams. The disruptions started early this morning and are believed to be the result of a cyberattack. https://brusselsmorning.com/technical-problems-disrupt-de-lijn-services-cyberattack-suspected/62618/
- ***Over 300K Prometheus Instances Exposed: Credentials and API Keys Leaking Online*** - Cybersecurity researchers are warning that thousands of servers hosting the Prometheus monitoring and alerting toolkit are at risk of information leakage and exposure to denial-of-service (DoS) as well as remote code execution (RCE) attacks. https://thehackernews.com/2024/12/296000-prometheus-instances-exposed.html
- ***Beyondtrust Says Hackers Breached Remote Support Saas Instances -*** Privileged access management company BeyondTrust suffered a cyberattack in early December after threat actors breached some of its Remote Support SaaS instances. https://www.bleepingcomputer.com/news/security/beyondtrust-says-hackers-breached-remote-support-saas-instances/
- ***Abrasive Supply Data Breach*** - Abrasive Supply specializes in abrasive products, including sanding discs, belts, and air tools for industrial sanding and grinding applications. https://www.breachsense.com/breaches/abrasive-supply-data-breach/

## SECURITY VULNERABILITIES, ALERTS, ADVISORIES, & UPDATES

### US CERT/ ICS CERT Alerts and Advisories

1. Acclaim Systems - https://www.cve.org/CVERecord?id=CVE-2021-44207

### SUSE Security Updates

1. aalto-xml, flatten-maven-plugin, jctools, moditect, netty, netty-tcnative - https://www.suse.com/support/update/announcement/2024/suse-su-20244407-1
2. vim - https://www.suse.com/support/update/announcement/2024/suse-su-20244409-1
3. amazon-dracut-config, google-dracut-config, microsoft-dracut-config - https://www.suse.com/support/update/announcement/2024/suse-ru-20244410-1
4. mozjs115 –
   a. https://www.suse.com/support/update/announcement/2024/suse-su-20244411-1
   b. https://www.suse.com/support/update/announcement/2024/suse-su-20244412-1

### Fedora Security Advisories

1. prometheus-podman-exporter –
   a. https://lwn.net/Articles/1003267
   b. https://lwn.net/Articles/1003268

### Check Point Security Advisories

1. Django - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-1169.html
2. Reolink - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2019-3245.html
3. Draytek Vigor2960 - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2023-1951.html
4. Apache - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-1154.html
5. NUU0 NVRmini - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2022-2160.html

email st-isac@surfacetransportationisac.org