Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

Daily Open-Source Cyber Report

December 17, 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

- U.S. Arrests Scattered Spider Suspect Linked To Telecom Hacks
- Internet-Exposed HMIs Pose Cybersecurity Risks to Water and Wastewater Systems
- 84 Arrested as Russian Ransomware Laundering Networks Disrupted
- Compromised Software Code Poses New Systemic Risk to U.S. Critical Infrastructure
- Transportation Companies Face Increasing Cyber Risks
- IoT Takes The Wheel: Telematics Is Transforming Construction
- Businesses Plagued By Constant Stream Of Malicious Emails

Emerging Threats & Vulnerabilities

- Redline Info-Stealer Campaign Targets Russian Businesses Through Pirated Corporate Software
- HiatusRAT Actors Targeting Web Cameras and DVRs
- Socks5Systemz Botnet Powers Illegal Proxy Service with 85,000+ Hacked Devices
- MC LR Router and GoCast unpatched vulnerabilities
- Update Now! Apple Releases New Security Patches For Vulnerabilities In Iphones, Macs, And More

Attacks, Breaches, & Leaks

- Tibber – 50,002 Breached Accounts
- 900,000 People Impacted by ConnectOnCall Data Breach
- Ultralytics AI Library with 60M Downloads Compromised for Cryptomining
- BU and Federal Investigation Underway into Hacking of Framingham Heart Study Data

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

EXECUTIVE NEWS

U.S. Arrests Scattered Spider Suspect Linked To Telecom Hacks
Bleeping Computer, 12/5/2024

U.S. authorities have arrested a 19-year-old teenager linked to the notorious Scattered Spider cybercrime gang who is now charged with breaching a U.S. financial institution and two unnamed telecommunications firms. Remington Goy Ogletree (also known online as "remi") breached the three companies' networks using credentials stolen in text and voice phishing messages targeting their employees. He also impersonated the victims' IT support departments in calls designed to pressure the employees into accessing phishing sites where they were asked to enter their user names and passwords. https://www.bleepingcomputer.com/news/security/us-arrests-scattered-spider-suspect-linked-to-telecom-hacks/

Internet-Exposed HMIs Pose Cybersecurity Risks to Water and Wastewater Systems
CISA, 12/13/2024

This joint fact sheet, created in collaboration with the Environmental Protection Agency (EPA), supplies Water and Wastewater Systems (WWS) facilities with recommendations for limiting the exposure of Human Machine Interfaces (HMIs) and securing them against malicious cyber activity. In the absence of cybersecurity controls, threat actors can exploit exposed HMIs at WWS Sector utilities to view the contents of the HMI, make unauthorized changes, and potentially disrupt the facility's water and/or wastewater treatment process. CISA strongly encourages WWS Sector organizations review and implement the mitigations in this fact sheet to harden remote access to HMIs.
https://www.cisa.gov/resources-tools/resources/internet-exposed-hmis-pose-cybersecurity-risks-water-and-wastewater-systems

84 Arrested as Russian Ransomware Laundering Networks Disrupted
Hack Read, 12/7/2024

A joint international effort led by the UK's National Crime Agency (NCA) has successfully disrupted two large-scale Russian-speaking criminal networks involved in laundering millions of dollars in illegal funds. Dubbed Operation Destabilise, the investigation exposed a network of financial transactions that supported various criminal activities, including ransomware attacks, drug trafficking, and Russian espionage. Two networks, identified as "Smart" (led by Ekaterina Zhdanova) and "TGR" (led by Rossi, Chirkinyan, and Bradens), were instrumental in facilitating the movement of illegal funds across borders, often using cryptocurrency as a primary tool. https://hackread.com/84-arrest-russia-ransomware-launder-network-disrupted/

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

Compromised Software Code Poses New Systemic Risk to U.S. Critical Infrastructure
Dark Reading, 12/5/2024

The code that makes up the software now powering U.S. utilities is rife with vulnerabilities, including hundreds that are "highly exploitable," a new research report released by Fortress Information Security today finds. Researchers studied thousands of products and found troubling risk patterns. The report, Beyond the Bill of Materials: The Silent Threat Lurking in Critical Infrastructure Software, also shows that 25 percent of software components and 90 percent of software products contained code from developers in China. Compromised software code can provide threat actors with a "backdoor" into power grids, oil and gas pipelines, and communication networks.
https://www.darkreading.com/application-security/compromised-software-code-poses-systemic-risks-to-critical-infrastructure

Transportation Companies Face Increasing Cyber Risks
S&P Global, 12/12/2024

Digitalization has transformed the global transportation sector, enabling the integration and streamlining of transport networks, slashing operating costs, and improving customers' experience. However, there is a flip side to those gains that can have implications for the credit quality of operators. Why it matters: The digital systems that facilitate trade and tourism flows are an enticing target for malevolent actors who know that a successful cyber attack could disrupt networks that are vital to the supply of goods, could inflict material economic damage, and are likely to be high profile.
https://www.spglobal.com/ratings/en/research/articles/241212-transportation-companies-face-increasing-cyber-risks-13334611

IoT Takes The Wheel: Telematics Is Transforming Construction
IoT News, 12/2/2024

The adoption of telematics systems in construction is gaining traction, with the installed base of active systems exceeding 6.8 million. IoT market research provider Berg Insight forecasts a compound annual growth rate (CAGR) of 12.0 percent for the active installed base, which is set to almost double to 12.1 million units worldwide by 2028. The figures encompass all construction equipment telematics solutions offered by OEMs, whether developed in-house or supplied through partnerships with third-party telematics providers. A regional breakdown reveals an estimated 900,000 active telematics systems in Europe as of 2023, with the North American market surpassing Europe in size. However, the bulk of the global installed base – more than 50 percent – comes from the "Rest of the World," which reflects surging adoption in emerging construction markets. https://iottechnews.com/news/iot-takes-wheel-telematics-transforming-construction/

Businesses Plagued By Constant Stream Of Malicious Emails
Help Net Security, 12/9/2024

36.9% of all emails received by businesses (20.5 billion) in 2024 were unwanted, according to Hornetsecurity's analysis of 55.6+ billion emails processed through their security services between November 1, 2023 and October 31, 2024 – and 2.3% of those contained malicious content, totalling 427.8 million emails. Once again, phishing remains the most prevalent form of attack, responsible for a third of all cyber-attacks in 2024. This was confirmed by the analysis of 55.6 billion emails, showing that phishing remains a top concern consistently year over year. Malicious URLs and advanced fee scams were responsible for 22.7% and 6.4% respectively. https://www.helpnetsecurity.com/2024/12/09/malicious-emails-inboxes/

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

TECHNICAL SUMMARY

EMERGING THREATS & EXPLOITS

- ***Redline Info-Stealer Campaign Targets Russian Businesses Through Pirated Corporate Software -*** Since January 2024, Russian businesses using unlicensed software have been targeted by an ongoing RedLine info-stealer campaign. Pirated software is distributed via Russian online forums, attackers disguise the malware as a tool to bypass licensing for business automation software. https://securityaffairs.com/171771/cyber-crime/redline-info-stealer-campaign-targets-russian-businesses.html
- ***HiatusRAT Actors Targeting Web Cameras and DVRs*** - The Federal Bureau of Investigation (FBI) is releasing this Private Industry Notification (PIN) to highlight HiatusRAT1 scanning campaigns against Chinese-branded web cameras and DVRs. Private sector partners are encouraged to implement the recommendations listed in the "Mitigation" column of the table below to reduce the likelihood and impact of these attack campaigns. https://www.ic3.gov/CSA/2024/241216.pdf
- ***Socks5Systemz Botnet Powers Illegal Proxy Service with 85,000+ Hacked Devices -*** A malicious botnet called Socks5Systemz is powering a proxy service called PROXY.AM, according to new findings from Bitsight. https://thehackernews.com/2024/12/socks5systemz-botnet-powers-illegal.html
- ***MC LR Router and GoCast unpatched vulnerabilities –*** Cisco Talos' Vulnerability Research team recently discovered two vulnerabilities in MC Technologies LR Router and three vulnerabilities in the GoCast service. These vulnerabilities have not been patched at time of this posting. https://blog.talosintelligence.com/mc-lr-router-and-gocast-zero-day-vulnerabilities-2/
- ***Update Now! Apple Releases New Security Patches For Vulnerabilities In Iphones, Macs, And More*** - Apple has released security patches for most of its operating systems, including iOS, Mac, iPadOS, Safari, and visionOS. https://www.malwarebytes.com/blog/apple/2024/12/update-now-apple-releases-new-security-patches-for-vulnerabilities-in-iphones-macs-and-more

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

ATTACKS, BREACHES & LEAKS

- ***Tibber – 50,002 Breached Accounts*** **-** In November 2024, the German electricity provider Tibber suffered a data breach that exposed the personal information of 50k customers. The data included names, email addresses, geographic locations (city and postcode) and total spend on purchases. The data was provided to HIBP by a source who requested it be attributed to "Threat Actor 888". https://www.redpacketsecurity.com/tibber-50-002-breached-accounts/
- ***900,000 People Impacted by ConnectOnCall Data Breach*** - ConnectOnCall is notifying more than 900,000 individuals that their personal information and medical information was compromised in a data breach earlier this year. https://www.securityweek.com/900000-people-impacted-by-connectoncall-data-breach/
- ***Ultralytics AI Library with 60M Downloads Compromised for Cryptomining*****-** The latest research from ReversingLabs (RL) shared with Hackread.com, reveals that a popular AI library called “Ultralytics“ has been secretly mining cryptocurrency for someone else. This follows the recent discovery of the malicious aiocpa Python package, which was spreading an infostealer. https://hackread.com/ultralytics-ai-library-compromised-for-cryptomining/
- ***BU and Federal Investigation Underway into Hacking of Framingham Heart Study Data*** - Boston University’s renowned Framingham Heart Study (FHS) was breached by hackers, who gained access to the data of participants—both living and deceased—of the country’s longest running, multigenerational heart study. https://www.bu.edu/articles/2024/investigation-into-hacking-of-fhs-data/

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. ThreatQuotient - https://www.cisa.gov/news-events/ics-advisories/icsa-24-352-01
2. Hitachi Energy - https://www.cisa.gov/news-events/ics-advisories/icsa-24-352-02
3. Rockwell Automation - https://www.cisa.gov/news-events/ics-advisories/icsa-24-352-03
4. Schneider Electric - https://www.cisa.gov/news-events/ics-advisories/icsa-24-352-04
5. BD Diagnostic - https://www.cisa.gov/news-events/ics-medical-advisories/icsma-24-352-01

SUSE Security Updates

1. Hwdata - https://www.suse.com/support/update/announcement/2024/suse-ru-20244363-1
2. yast2-network - https://www.suse.com/support/update/announcement/2024/suse-ru-20244362-1
3. gdm – https://www.suse.com/support/update/announcement/2024/suse-ru-20244361-1
4. docker - https://www.suse.com/support/update/announcement/2024/suse-su-20244360-1
5. curl - https://www.suse.com/support/update/announcement/2024/suse-su-20244359-1
6. python-urllib3_1 - https://www.suse.com/support/update/announcement/2024/suse-su-20244358-1
7. ovmf - https://www.suse.com/support/update/announcement/2024/suse-su-20244357-1

Fedora Security Advisories

1. python-notebook - https://lwn.net/Articles/1002464
2. jupyterlab –
    a. https://lwn.net/Articles/1002462
    b. https://lwn.net/Articles/1002463

Check Point Security Advisories

1. Adobe - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-0187.html
2. Microsoft - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-0371.html

Red Hat Security Advisories

1. containernetworking-plugins - https://access.redhat.com/errata/RHSA-2024:11216
2. skopeo - https://access.redhat.com/errata/RHSA-2024:11217
3. edk2:20240524 - https://access.redhat.com/errata/RHSA-2024:11219
4. unbound:1.16.2 - https://access.redhat.com/errata/RHSA-2024:11232
5. libsndfile:1.0.31 - https://access.redhat.com/errata/RHSA-2024:11237
6. python3.11-urllib3 - https://access.redhat.com/errata/RHSA-2024:11238
7. pam - https://access.redhat.com/errata/RHSA-2024:11250

Oracle Linux Security Update

1. postgresql –
    a. https://lwn.net/Articles/1002475
    b. https://lwn.net/Articles/1002474
2. Kernel –
    a. https://lwn.net/Articles/1002472
    b. https://lwn.net/Articles/1002470
3. gimp:2.8.22 –
    a. https://lwn.net/Articles/1002466
    b. https://lwn.net/Articles/1002467
4. gstreamer1-plugins-good - https://lwn.net/Articles/1002469
5. gstreamer1-plugins-base - https://lwn.net/Articles/1002468