Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

Daily Open-Source Cyber Report

December 2, 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

- National Security Agency publishes OT Cybersecurity Guidance
- Russia-Linked Threat Actors Threaten The UK And Its Allies, Minister To Say
- Operation Shipwrecked: U.S. Seizes PopeyeTools Marketplace, Charges 3
- Active Network Of North Korean IT Front Companies Exposed
- Meta Cracks Down On Millions Of Accounts It Tied To Pig-Butchering Scams
- Navigating the Ethical Dilemmas of Vehicular Communication for Transportation Safety
- How To Protect The Global Supply Chain From Phishing Scams

Emerging Threats & Vulnerabilities

- Chinese APT Gelsemium Targets Linux Systems with New WolfsBane Backdoor
- Recent Zyxel Firewall Vulnerability Exploited in Ransomware Attacks
- Hackers Abuse Avast Anti-Rootkit Driver To Disable Defenses
- Russian Cyber Spies Target Organizations with HatVibe and CherrySpy Malware
- Faux ChatGPT, Claude API Packages Deliver JarkaStealer

Attacks, Breaches, & Leaks

- Ransomware Attack on Berexco LLC: A Detailed Analysis
- ADT Freight Services Australia
- Hoboken City Hall Gets Hacked With Ransomware, They Say
- UK hospital network postpones procedures after cyberattack

EXECUTIVE NEWS

National Security Agency publishes OT Cybersecurity Guidance
Cyber Scoop, 11/25/2024

As the digital world continuously evolves, cybersecurity professionals are becoming increasingly concerned about attacks on operational technology in the transportation sector. Electronic control units (ECU) are everywhere, from planes to automobiles, including large trucks that have the potential to be shut down because a hacker found an avenue in via GPS, for example. That could cause supply chain issues if it's a common control unit and the manufacturer decides to issue a patch or some kind of fix, pulling those trucks off the road, impacting operational uptime, said Jeff Hall, principal security consultant and North American aerospace lead at cybersecurity consulting firm NCC Group.
https://www.ccjdigital.com/technology/cybersecurity/article/15708230/national-security-agency-publishes-ot-cybersecurity-guidance

Russia-Linked Threat Actors Threaten The UK And Its Allies, Minister To Say
Security Affairs, 11/25/2024

Russia may launch cyberattacks against the UK and its allies in retaliation for their support of Ukraine, Chancellor of the Duchy of Lancaster Pat McFadden is expected to state during a NATO meeting. Chancellor of the Duchy of Lancaster Pat McFadden is also responsible for National security, resilience, and civil contingencies. According to the BBC, he believes that Russia is conducting a "hidden war" against the UK and its allies. He is expected to warn about the activity conducted by Russia's GRU Unit 29155, which the UK government accuses of conducting several attacks across the UK and Europe.
https://securityaffairs.com/171357/intelligence/russia-linked-threat-actors-threaten-uk.html

Operation Shipwrecked: U.S. Seizes PopeyeTools Marketplace, Charges 3
Hack Read, 11/21/2024

The US Department of Justice (DoJ) has seized and shut down PopeyeTools, a notorious online marketplace that facilitated a wide range of illegal activities, and arrested three alleged administrators of the website. PopeyeTools was operational since at least 2016, and functioned as a hub for cybercriminals, offering stolen financial data, tools for carrying out fraud, and even tutorials on how to commit these crimes. The three men charged, Abdul Ghaffar (Pakistan), Abdul Sami (Pakistan), and Javed Mirza (Afghanistan), face up to 10 years in prison each for access device fraud charges levied against them. This move is part of the department's "all-tools" approach to combating cybercrime.
https://hackread.com/us-seized-popeyetools-marketplace-chrges-3/

Active Network Of North Korean IT Front Companies Exposed

Help Net Security, 11/21/2024

US authorities have been warning about North Korean IT workers' tactics to bypass sanctions for a number of years, and have repeatedly seized website domains that looked like they belong to legitimate IT services companies and were used to help North Korean IT workers to hide their true identities and location when applying for jobs. They've also disrupted US-based schemes aimed at facilitating their employment and perpetrating the deception. SentinelOne researchers have analyzed the websites of four recently identified front companies (whose domains have been seized), and have uncovered multiple leads that point to an active network of North Korean IT front companies originating in China. https://www.helpnetsecurity.com/2024/11/21/north-korean-it-front-companies/

Meta Cracks Down On Millions Of Accounts It Tied To Pig-Butchering Scams

Cyber Scoop , 11/21/2024

Facebook and Instagram parent company Meta has taken down millions of accounts this year linked to overseas scam centers that enable a kind of cyber-related, fast-growing fraud known as "pig butchering," the social media giant said Thursday. The account takedowns are part of a multifaceted Meta strategy to combat scams that have cost U.S. victims billions of dollars of losses in recent years, and the result of two years' worth of efforts from the company. "Pig butchering" is so named because it involves the metaphorical "fattening up" of victims by building up trust under false pretenses before they eventually, unwittingly hand over their money to the criminals perpetuating it. https://cyberscoop.com/meta-cracks-down-on-millions-of-accounts-it-tied-to-pig-butchering-scams/

Navigating the Ethical Dilemmas of Vehicular Communication for Transportation Safety

ER Times, 11/20/2024

Vehicle-to-everything (V2X) technology connects all road users to enhance road safety and improve traffic efficiency through direct communication. Network-based communication, or vehicle-to-network-to-everything (V2N2X), aims to support some V2X use cases by transmitting data through the cellular network to multiple cloud servers. Examining the ethical aspects of both V2X and V2N2X provides new insights into their respective characteristics. Ethical implementation of these technologies necessitates strong measures to anonymize data and prevent unauthorized access, ensuring that data is solely used for safety and efficiency and not for surveillance or commercial purposes without consent. V2X is designed with these requirements in mind, using random and frequently changing identifiers for road users. https://www.eetimes.eu/navigating-the-ethical-dilemmas-of-vehicular-communication-for-transportation-safety/

How To Protect The Global Supply Chain From Phishing Scams
Tank Transport, 11/25/2024

The supply chain is a highly interconnected ecosystem of suppliers, manufacturers, logistics, retailers and finally, consumers. The exchange of goods and the flow of transportation between all of these various groups is the backbone of our global economy. But if disrupted, our interconnected world could face all types and levels of chaos – from stolen Christmas presents to empty shelves in grocery stores or hospitals being unable to get their hands on life-saving supplies. It is imperative that organizations prepare for significant cyber incidents. A new white paper from the World Economic Forum, in collaboration with the University of Oxford, unpacks the concept of cyber resilience, outlining the evolution of the cyber paradigm and highlighting that cyber resilience is an organization's ability to minimize the impact of significant cyber incidents on its primary goals and objectives.
https://www.weforum.org/stories/2024/11/protect-global-supply-chain-from-phishing-scams/

TECHNICAL SUMMARY

EMERGING THREATS & EXPLOITS

- ***Chinese APT Gelsemium Targets Linux Systems with New WolfsBane Backdoor -*** The China-aligned advanced persistent threat (APT) actor known as Gelsemium has been observed using a new Linux backdoor dubbed WolfsBane as part of cyber attacks likely targeting East and Southeast Asia. https://thehackernews.com/2024/11/chinese-apt-gelsemium-targets-linux.html
- ***Recent Zyxel Firewall Vulnerability Exploited in Ransomware Attacks*** - Zyxel has issued a fresh warning on threat actors exploiting a recently patched command injection vulnerability in its firewalls after security firms have observed a ransomware group targeting the flaw for initial compromise. https://www.securityweek.com/recent-zyxel-firewall-vulnerability-exploited-in-ransomware-attacks/
- ***‘Hackers Abuse Avast Anti-Rootkit Driver To Disable Defenses –*** A new malicious campaign is using a legitimate but old and vulnerable Avast Anti-Rootkit driver to evade detection and take control of the target system by disabling security components. The malware that drops the driver is a variant of an AV Killer of no particular family. It comes with a hardcoded list of 142 names for security processes from various vendors. https://www.bleepingcomputer.com/news/security/hackers-abuse-avast-anti-rootkit-driver-to-disable-defenses/
- ***Russian Cyber Spies Target Organizations with HatVibe and CherrySpy Malware –*** A Russian-aligned hacking group is conducting a cyber espionage campaign across Europe and Asia, according to Recorded Future. Insikt Group, Recorded Future’s threat intelligence team, has shared in a November 21 report that a group it tracks as TAG-110 has been using custom malware to compromise government entities, human rights groups and educational institutions. https://www.infosecurity-magazine.com/news/russian-cyber-spies-hatvibe/
- ***Faux ChatGPT, Claude API Packages Deliver JarkaStealer -*** Two Python packages claiming to integrate with popular chatbots actually transmit an infostealer to potentially thousands of victims. Publishing open source packages with malware hidden inside is a popular way to infect application developers, and the organizations they work for or serve as customers. https://www.darkreading.com/application-security/faux-chatgpt-claude-api-packages-jarkastealer

ATTACKS, BREACHES & LEAKS

- ***Ransomware Attack on Berexco LLC: A Detailed Analysis*** **-** In a significant cybersecurity incident, Berexco LLC, an independent oil and gas exploration and production company based in Wichita, Kansas, has fallen victim to a ransomware attack orchestrated by the Akira group. This attack underscores the vulnerabilities faced by companies in the energy sector, particularly those with extensive operational footprints and sensitive data. https://www.halcyon.ai/attacks/berexco-llc-hit-by-akira-ransomware-exposing-sensitive-data
- ***ADT Freight Services Australia*** - ADT Freight Services Australia Pty Ltd is a Melbourne-based international freight forwarder and customs agency, specializing in air, sea, and road transportation, including motor vehicles. https://www.halcyon.ai/attacks/meow-group-ransomware-hits-equator-worldwide-data-breach-alert
- ***Hoboken City Hall Gets Hacked With Ransomware, They Say*** **-** Hoboken residents received an alert shortly after 10 a.m. Wednesday saying City Hall offices are closed as a result of a "cyber attack." The city says that the offices will remain closed for the day, and street sweeping is suspended. https://patch.com/new-jersey/hoboken/hoboken-city-hall-victim-cyber-attack-they-say-messages
- ***UK Hospital Network Postpones Procedures After Cyberattack*** - Major UK healthcare provider Wirral University Teaching Hospital (WUTH), part of the NHS Foundation Trust, has suffered a cyberattack that caused a systems outage leading to postponing appointments and scheduled procedures. https://www.bleepingcomputer.com/news/security/uk-hospital-network-postpones-procedures-after-cyberattack/

SECURITY VULNERABILITIES, ALERTS, ADVISORIES, & UPDATES

SUSE Security Updates

1. nodejs18 - https://www.suse.com/support/update/announcement/2024/suse-ru-20244113-1
2. postgresql13 - https://www.suse.com/support/update/announcement/2024/suse-su-20244114-1
3. gtk4 - https://www.suse.com/support/update/announcement/2024/suse-ru-20244115-1
4. xen - https://www.suse.com/support/update/announcement/2024/suse-su-20244116-1
5. webkit2gtk3 - https://www.suse.com/support/update/announcement/2024/suse-su-20244117-1
6. postgresql14 - https://www.suse.com/support/update/announcement/2024/suse-su-20244118-1
7. Dracut - https://www.suse.com/support/update/announcement/2024/suse-ru-20244130-1
8. Linux Kernel - https://www.suse.com/support/update/announcement/2024/suse-su-20244131-1
9. Mariadb –
   a. https://www.suse.com/support/update/announcement/2024/suse-ru-20244133-1
   b. https://www.suse.com/support/update/announcement/2024/suse-ru-20244132-1
10. python-tornado6 - https://www.suse.com/support/update/announcement/2024/suse-su-20244137-1
11. wget - https://www.suse.com/support/update/announcement/2024/suse-su-20244138-1

Fedora Security Advisories

1. wireshark –
   a. https://lwn.net/Articles/1000454
   b. https://lwn.net/Articles/1000453
2. Qbittorrent - https://lwn.net/Articles/1000451
3. Webkitgtk - https://lwn.net/Articles/1000452
4. rust-zlib-rs - https://lwn.net/Articles/1000167
5. rust-rustls - https://lwn.net/Articles/1000164
6. firefox - https://lwn.net/Articles/1000161
7. rust-rustls - https://lwn.net/Articles/1000165

Mageia Security Advisories

1. krb5 - http://advisories.mageia.org/MGASA-2024-0385.html
2. thunderbird, thunderbird-l10n - http://advisories.mageia.org/MGASA-2024-0384.html
3. rootcerts, nss, firefox, firefox-l10n - http://advisories.mageia.org/MGASA-2024-0383.html
4. libsoup3, libsoup - http://advisories.mageia.org/MGASA-2024-0382.html
5. lxqt-menu-data - http://advisories.mageia.org/MGAA-2024-0233.html

Debian Security Advisories

1. simplesamlphp - https://lists.debian.org/debian-security-announce/2024/msg00237.html

Check Point Security Advisories

1. Haxx - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-1071.html
2. Tenda - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-1090.html
3. Apache - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2023-1937.html
4. Ivanti - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-1062.html
5. ProjectSend - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-1108.html
6. Squid Denial of Service - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-0144.html

Drupal Security Notices

1. Tarte au Citron - https://www.drupal.org/sa-contrib-2024-064

Red Hat Security Advisories

1. Libreswan - https://access.redhat.com/errata/RHSA-2024:10594
2. Postgresql - https://access.redhat.com/errata/RHSA-2024:10595
3. gimp:2.8.22 - https://access.redhat.com/errata/RHSA-2024:10666
4. thunderbird - https://access.redhat.com/errata/RHSA-2024:10667
5. postgresql:13 - https://access.redhat.com/errata/RHSA-2024:10677
6. firefox - https://access.redhat.com/errata/RHSA-2024:10702

Ubuntu Security Notices

2. Ansible - https://ubuntu.com/security/notices/USN-6846-2