Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

Daily Open-Source Cyber Report

December 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.

AT-A-GLANCE

Executive News

- Notorious Ransomware Developer Charged With Computer Crimes In Russia
- Chinese LIDAR Dominance a Cybersecurity Threat, Warns Think Tank
- Source Code of $3,000-a-Month macOS Malware 'Banshee Stealer' Leaked
- Driverless Semi Company Pumps The Brakes, Delays Texas Launch
- BlackBasta Ransomware Brand Picks Up Where Conti Left Off
- VPN Vulnerabilities, Weak Credentials Fuel Ransomware Attacks
- Why Cybersecurity Leaders Trust the MITRE ATT&CK Evaluations

Emerging Threats & Vulnerabilities

- 'Matrix' Hackers Deploy Massive New IoT Botnet for DDoS Attacks
- New Bootkit "Bootkitty" Targets Linux Systems via UEFI
- VMware Patches High-Severity Vulnerabilities in Aria Operations
- Hackers exploit ProjectSend Flaw To Backdoor Exposed Servers
- APT-C-60 Hackers Exploit StatCounter and Bitbucket in SpyGlace Malware Campaign

Attacks, Breaches, & Leaks

- Data Broker Exposes 600,000 Sensitive Files Including Background Checks
- Ransomware gang BlackSuit says it hacked Alabama county government
- Schuck Group GmbH Faces Ransomware Threat from INC Ransom
- BT Unit Took Servers Offline After Black Basta Ransomware Breach
- Vodka Giant Stoli Files for Bankruptcy After Ransomware Attack

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

EXECUTIVE NEWS

Notorious Ransomware Developer Charged With Computer Crimes In Russia
Cyber Scoop, 12/2/2024

Russian authorities have charged Mikhail Matveev, a notorious hacker known as Wazawaka, for creating malware used to extort commercial organizations, the Russian Interior Ministry announced last week. Matveev, linked to ransomware groups such as Babuk, Conti, DarkSide, Hive, and LockBit, faces charges under Russia's Criminal Code for the creation or distribution of software intended to damage or manipulate information systems. If convicted, Matveev could be sentenced to up to four years in prison or fined. The developments were first reported by the Russian state news agency RIA Novosti. Subsequently, a cybersecurity-focused online community known as "club1337" claimed to have contacted Wazawaka, who confirmed the charges. Matveev reportedly admitted to paying two fines and having a large amount of his cryptocurrency seized. https://cyberscoop.com/mikhail-matveev-wazawaka-russia-charges/

Chinese LIDAR Dominance a Cybersecurity Threat, Warns Think Tank
Infosecurity Magazine, 12/3/2024

An over-reliance on Chinese-made remote sensing technology could imperil US national, economic and cyber security, a think tank has warned. The non-profit Foundation for Defense of Democracies (FDD) argued in a new paper published yesterday that US critical national infrastructure (CNI) providers in sectors like public safety, transportation and utility are particularly exposed to Chinese light detection and ranging (LIDAR) technology. LIDAR uses laser light to rapidly create highly accurate 3D maps and models and is now indispensable in a wide range of military and civilian use cases, including safe navigation for autonomous vehicles, drones and trains, and monitoring of pipelines, power lines and rail networks, FDD claimed. On the battlefield, it's also used for critical tasks like enemy detection, navigation and sea mine detection, the report noted. https://www.infosecurity-magazine.com/news/chinese-lidar-dominance/

Source Code of $3,000-a-Month macOS Malware 'Banshee Stealer' Leaked
Security Week, 11/27/2024

Threat intelligence and research project Vx-Underground reported this week that the Banshee Stealer source code was leaked online. The project said the malware operation has been shut down as a result of the leak. It's unclear who leaked the code and why. Vx-Underground has made the Banshee Stealer source code available on its GitHub account. Banshee Stealer made many headlines in August, after its developers started advertising it on cybercrime forums for a monthly subscription of $3,000.
https://www.securityweek.com/source-code-of-3000-a-month-macos-malware-banshee-stealer-leaked/

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

Driverless Semi Company Pumps The Brakes, Delays Texas Launch
Transit Talent, 11/27/2024

It'll be a little longer before drivers begin sharing the road with semis with no human on board. The self-driving tech company Aurora Innovation has delayed its driverless truck launch in Texas until next year. Texas has been a testing ground for driverless semis for years. “They have had self-driving 18-wheelers up and down I-45, across I-30, across I-20 for several years, but they have a human in the seat. So they still have a human in the seat in case something goes awry,” said Amy Witherite, founder of Witherite Law Group and traffic safety advocate. https://www.nbcdfw.com/news/local/driverless-semi-company-delays-texas-launch/3708940/

BlackBasta Ransomware Brand Picks Up Where Conti Left Off
Dark Reading, 11/25/2024

The Russian-language ransomware scene isn't all that big. And despite an array of monikers for individual operations, new analysis shows these groups' members are working in close coordination, sharing tactics, botnets, and malware among one another, as well as with the Russian state. And now, a new power player ransomware group brand has emerged — BlackBasta. Since the spectacular law enforcement takedown of Conti's operations in 2022, the Russian-language ransomware landscape has been a bit in flux. Upending usual business operations further was the subsequent August 2023 takedown of Qakbot botnets, long relied upon by these groups to deliver their ransomware. https://www.darkreading.com/vulnerabilities-threats/blackbasta-ransomware-group-conti

VPN Vulnerabilities, Weak Credentials Fuel Ransomware Attacks
Help Net Security, 11/28/2024

Attackers leveraging virtual private network (VPN) vulnerabilities and weak passwords for initial access contributed to nearly 30% of ransomware attacks, according to Corvus Insurance. According to the Q3 report, many of these incidents were traced to outdated software or VPN accounts with inadequate protection. For example, common usernames such as “admin” or “user” and a lack of multi-factor authentication (MFA) made accounts vulnerable to automated brute-force attacks, where attackers exploit publicly accessible systems by testing combinations of these weak credentials, frequently achieving network access with minimal effort. https://www.engineerlive.com/content/digital-rail-solutions-are-more-vital-ever

Why Cybersecurity Leaders Trust the MITRE ATT&CK Evaluations
Bleeping Computer, 11/26/2024

In today's dynamic threat landscape, security leaders are under constant pressure to make informed choices about which solutions and strategies they employ to protect their organizations. The "MITRE Engenuity ATT&CK Evaluations: Enterprise" stand out as an essential resource for cybersecurity decision makers to navigate this challenge. Unlike other independent assessments, MITRE ATT&CK Evaluations simulate real-world threats to assess how competing cybersecurity vendors detect and respond to real-world threats. As soon as the highly anticipated 2024 MITRE ATT&CK Evaluation results are released, this webinar will distill key findings for cybersecurity leaders.
https://www.bleepingcomputer.com/news/security/why-cybersecurity-leaders-trust-the-mitre-attack-evaluations/

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

TECHNICAL SUMMARY

EMERGING THREATS & EXPLOITS

- ***'Matrix' Hackers Deploy Massive New IoT Botnet for DDoS Attacks -*** Aqua Nautilus researchers have discovered a campaign powering a series of large-scale DDoS attacks launched by Matrix, which could be a Russian threat actor. Learn about the vulnerabilities exploited, the techniques used, and the possible impact on businesses worldwide. https://hackread.com/matrix-hackers-new-iot-botnet-ddos-attacks/
- ***New Bootkit "Bootkitty" Targets Linux Systems via UEFI*** - Cybersecurity researchers have discovered "Bootkitty," possibly the first UEFI bootkit specifically designed to target Linux systems. This marks a significant shift in the UEFI threat landscape, which previously focused exclusively on Windows-based attacks. https://www.helpnetsecurity.com/2024/11/26/romcom-backdoor-cve-2024-9680-cve-2024-49039/
- ***VMware Patches High-Severity Vulnerabilities in Aria Operations -*** The company documented five distinct vulnerabilities in the cloud IT operations platform and warned that malicious hackers can craft exploits to elevate privileges or launch cross-site scripting attacks. https://www.securityweek.com/vmware-patches-high-severity-vulnerabilities-in-aria-operations/
- ***Hackers exploit ProjectSend Flaw To Backdoor Exposed Servers –*** Threat actors are using public exploits for a critical authentication bypass flaw in ProjectSend to upload webshells and gain remote access to servers. https://www.bleepingcomputer.com/news/security/hackers-exploit-projectsend-flaw-to-backdoor-exposed-servers/
- ***APT-C-60 Hackers Exploit StatCounter and Bitbucket in SpyGlace Malware Campaign -*** The threat actor known as APT-C-60 has been linked to a cyber attack targeting an unnamed organization in Japan that used a job application-themed lure to deliver the SpyGlace backdoor. https://thehackernews.com/2024/11/apt-c-60-exploits-wps-office.html

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

ATTACKS, BREACHES & LEAKS

- ***Data Broker Exposes 600,000 Sensitive Files Including Background Checks -*** A researcher has discovered a data broker had stored 644,869 PDF files in a publicly accessible cloud storage container. The 713.1 GB container (an Amazon S3 bucket) did not have password-protection, and the data was left unencrypted, so anybody who stumbled on them could read the files. https://www.malwarebytes.com/blog/news/2024/11/data-broker-exposes-600000-sensitive-files-including-background-checks
- ***Ransomware Gang Blacksuit Says It Hacked Alabama County Government*** - Ransomware gang BlackSuit claimed responsibility for cyber attack earlier this month on the Cullman County Commission in Alabama. https://www.comparitech.com/news/ransomware-gang-blacksuit-says-it-hacked-alabama-county-government/
- ***Schuck Group GmbH Faces Ransomware Threat from INC Ransom -*** Schuck Group GmbH, a prominent manufacturer based in Germany, has fallen victim to a ransomware attack orchestrated by the INC Ransom group. The attack, which was first detected on November 23, 2024, has exposed the organization to significant data breaches and potential financial losses. https://www.halcyon.ai/attacks/schuck-group-gmbh-faces-ransomware-threat-from-inc-ransom
- ***BT Unit Took Servers Offline After Black Basta Ransomware Breach*** - Multinational telecommunications giant BT Group (formerly British Telecom) has confirmed that its BT Conferencing business division shut down some of its servers following a Black Basta ransomware breach. https://www.bleepingcomputer.com/news/security/bt-conferencing-division-took-servers-offline-after-black-basta-ransomware-attack/
- ***Vodka Giant Stoli Files for Bankruptcy After Ransomware Attack*** - A storied Russian vodka maker has filed for bankruptcy in the US just months after it was breached by ransomware actors. Stoli Group USA and Kentucky Owl (KO) CEO, Chris Caldwell, revealed in a legal filing that the group is around $78 million debt. https://www.infosecurity-magazine.com/news/vodka-stoli-bankruptcy-ransomware/

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. AutomationDirect C-More - https://www.cisa.gov/news-events/ics-advisories/icsa-24-340-01
2. Planet Technology - https://www.cisa.gov/news-events/ics-advisories/icsa-24-340-02

SUSE Security Updates

1. docker-stable - https://www.suse.com/support/update/announcement/2024/suse-su-20244205-1
2. rubygem-nokogiri - https://www.suse.com/support/update/announcement/2024/suse-ru-20244203-1
3. java-1_8_0-openjdk - https://www.suse.com/support/update/announcement/2024/suse-su-20244202-1
4. libsolv, libzypp, zipper - https://www.suse.com/support/update/announcement/2024/suse-ru-20244200-1
5. python-python-multipart - https://www.suse.com/support/update/announcement/2024/suse-su-20244194-1
6. lshw - https://www.suse.com/support/update/announcement/2024/suse-ru-20244190-1

Fedora Security Advisories

1. thunderbird - https://lwn.net/Articles/1000831
2. webkitgtk - https://lwn.net/Articles/1000833
3. tuned - https://lwn.net/Articles/1000832

Check Point Security Advisories

1. Apache –
    a. https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-0663.html
    b. https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2023-1422.html
2. HP Universal - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2014-2552.html

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

Red Hat Security Advisories

1. Firefox - https://access.redhat.com/errata/RHSA-2024:10844
2. postgresql:13 - https://access.redhat.com/errata/RHSA-2024:10846
3. ruby:2.5 - https://access.redhat.com/errata/RHSA-2024:10850
4. postgresql:15 - https://access.redhat.com/errata/RHSA-2024:10851
5. ruby - https://access.redhat.com/errata/RHSA-2024:10858
6. ruby:3.1 - https://access.redhat.com/errata/RHSA-2024:10860

Ubuntu Security Notices

1. Ghostscripts - https://ubuntu.com/security/notices/USN-7138-1
2. Apache Shiro - https://ubuntu.com/security/notices/USN-7139-1

Oracle Linux Security Update

1. postgresql:16 - https://lwn.net/Articles/1000850
2. python3:3.6.8 - https://lwn.net/Articles/1000852
3. krb5 - https://lwn.net/Articles/1000847
4. python-tornado - https://lwn.net/Articles/1000851
5. java-11-openjdk - https://lwn.net/Articles/1000842

Other

1. Google Chrome –
    a. https://chromereleases.googleblog.com/2024/12/chrome-dev-for-desktop-update.html
    b. https://chromereleases.googleblog.com/2024/12/chrome-stable-for-ios-update_90.html