Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

Daily Open-Source Cyber Report

December 18, 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. Charges Chinese Hacker for Exploiting Zero-Day in 81,000 Sophos Firewalls
- Phishers Impersonating Police Arrested in Multi-Million Euro Scam
- Cleo File Transfer Tool Vulnerability Exploited in Wild Against Enterprises
- Is KillSec3 Trying to Extort Victims Using Publicly Leaked Data?
- Fleets, Insurers Face Big Unknowns In The Transition To Autonomous Trucks
- Qr Codes Bypass Browser Isolation For Malicious C2 Communication
- Tips for Preventing Breaches in 2025

Emerging Threats & Vulnerabilities

- Researchers: Iranian Custom Malware Targets Fuel Systems
- Critical OpenWrt Flaw Exposes Firmware Update Server to Exploitation
- Critical Windows Zero-Day Alert: No Patch Available Yet for Users
- Microsoft NTLM Zero-Day to Remain Unpatched Until April
- Researchers Uncover Prompt Injection Vulnerabilities in DeepSeek and Claude AI

Attacks, Breaches, & Leaks

- Major Auto Parts Firm LKQ Hit by Cyberattack
- Sensitive Data Leaked After Namibia Ransomware Hack
- Certified Information Security Ransomware Breach by Bashe Group
- Texas Tech University System data breach impacts 1.4 million patients
- Canadian Eyecare Firm Care1 Exposes 2.2TB of Patient Records

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

EXECUTIVE NEWS

U.S. Charges Chinese Hacker for Exploiting Zero-Day in 81,000 Sophos Firewalls
The Hacker News, 12/11/2024

The U.S. government on Tuesday unsealed charges against a Chinese national for allegedly breaking into thousands of Sophos firewall devices globally in 2020.Guan Tianfeng (aka gbigmao and gxiaomao), who is said to have worked at Sichuan Silence Information Technology Company, Limited, has been charged with conspiracy to commit computer fraud and conspiracy to commit wire fraud. Guan has been accused of developing and testing a zero-day security vulnerability used to conduct the attacks against Sophos firewalls. "Guan Tianfeng is wanted for his alleged role in conspiring to access Sophos firewalls without authorization, cause damage to them, and retrieve and exfiltrate data from both the firewalls themselves and the computers behind these firewalls," the U.S. Federal Bureau of Investigation (FBI) said. "The exploit was used to infiltrate approximately 81,000 firewalls." .
https://thehackernews.com/2024/12/us-charges-chinese-hacker-for.html

Phishers Impersonating Police Arrested in Multi-Million Euro Scam
Hack Read, 12/9/2024

A massive phishing operation that targeted victims across Europe has been dismantled, thanks to a joint effort by Belgian and Dutch authorities, with the support of Europol. The operation, which is believed to have caused economic damages of several million euros, involved a gang of scammers who used phone and online phishing tactics to target victims in at least 10 European countries. The scammers, who were mostly based in the Netherlands, would pose as police or banking staff and approach older victims at their doors. The scammers used multiple tactics to target their victims including the following:
https://hackread.com/phishers-impersonate-police-arrest-million-euro-scam/

Cleo File Transfer Tool Vulnerability Exploited in Wild Against Enterprises
Security Week, 12/10/2024

Cleo is an Illinois-based company that provides supply chain and B2B integration solutions to more than 4,200 organizations. The firm informed customers in late October that it had patched an unrestricted file upload/download issue that could lead to remote code execution. The vulnerability, tracked as CVE-2024-50623, impacts Cleo Harmony, VLTrader, and LexiCom file transfer products, and it was supposed to be fixed with the release of version 5.8.0.21. However, Huntress determined that version 5.8.0.21 has failed to properly patch CVE-2024-50623, and discovered that threat actors have been exploiting the vulnerability in the wild. https://www.securityweek.com/cleo-file-transfer-tool-vulnerability-exploited-in-wild-against-enterprises/

Is KillSec3 Trying to Extort Victims Using Publicly Leaked Data?
Data Breaches, 12/8/2024

A recent report by SpyCloud indicated that nearly a third of companies that fell victim to ransomware last year had at least one infostealer infection in the 16 weeks prior to their attack. But correlation does not prove causation, and stolen credentials may not be the explanation for any one ransomware group's attacks. Today we consider another possible explanation for at least one group's attacks. A recent report by SpyCloud indicated that nearly a third of companies that fell victim to ransomware last year had at least one infostealer infection in the 16 weeks prior to their attack.
https://databreaches.net/2024/12/08/is-killsec3-trying-to-extort-victims-using-publicly-leaked-data/

Fleets, Insurers Face Big Unknowns In The Transition To Autonomous Trucks
Trucking Dive, 12/12/2024

Gatik is doubling down on autonomous trucks for the middle mile, aiming to mass produce AVs in 2027. Aurora plans to go fully autonomous in Q2 2025 for its Dallas-to-Houston launch lane. As AVs take to the roads, the trucking industry has a key question: how to insure these vehicles. Timothy Good, president of Good's Insurance Agency, said large trucking fleets are starting to prepare by studying and gathering as much data as possible on AVs. But plenty of questions remain unanswered, like whether premiums will go up or down, how risk will be assessed, and who or what is to blame in a crash.
https://www.truckingdive.com/news/av-insurance-premiums-future/735339/

Qr Codes Bypass Browser Isolation For Malicious C2 Communication
Bleeping Computer, 12/8/2024

Mandiant has identified a novel method to bypass browser isolation technology and achieve command-and-control operations through QR codes. Browser isolation is an increasingly popular security technology that routes all local web browser requests through remote web browsers hosted in a cloud environment or virtual machines. Any scripts or content on the visited web page is executed on the remote browser rather than the local one. The rendered pixel stream of the page is then sent back to the local browser that made the original request, only displaying what the page looks like and protecting the local device from any malicious code. https://www.bleepingcomputer.com/news/security/qr-codes-bypass-browser-isolation-for-malicious-c2-communication/

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

Tips for Preventing Breaches in 2025
Dark Reading, 12/11/2024

We witnessed some of the largest data breaches in recent history in 2024, with victims including industry titans like AT&T, Snowflake (and, therefore, Ticketmaster), and more. For US businesses, data breaches cost more than $9 million on average, and they cause lasting damage to customer and partner trust. Still, a resounding 98% of companies work with vendors that have had a breach. While business leaders have become more cautious in identifying vendors, they're integral to the growth of a business — providing critical goods, services, and technology to support ever-evolving business models and complex supply chains. https://www.darkreading.com/cyberattacks-data-breaches/tips-preventing-breaches-2025

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

TECHNICAL SUMMARY

EMERGING THREATS & EXPLOITS

- ***Researchers: Iranian Custom Malware Targets Fuel Systems -*** Researchers from New York-based Claroty said Friday that an attack wave from an Islamic Revolutionary Guard Corps-affiliated group going by the persona "CyberAv3ngers" swept up fuel management systems made by U.S.-based firm Gilbarco Veeder-Root. Claroty dubs the malware "IOControl." https://www.bankinfosecurity.com/researchers-iranian-custom-malware-targets-fuel-systems-a-27058
- ***Critical OpenWrt Flaw Exposes Firmware Update Server to Exploitation*** - The OpenWrt Project, an open-source initiative providing a Linux-based operating system for embedded devices, has pushed a critical patch to cover flaws that expose its firmware update server to malicious exploitation. https://www.securityweek.com/critical-openwrt-flaw-exposes-firmware-update-server-to-exploitation/
- ***Critical Windows Zero-Day Alert: No Patch Available Yet for Users -*** Protect your systems with automated patching and server hardening strategies to defend against vulnerabilities like the NTLM zero-day. Stay proactive and secure your business. https://hackread.com/windows-zero-day-alert-no-patch-available-for-users/
- ***Microsoft NTLM Zero-Day to Remain Unpatched Until April –*** Microsoft has released fresh guidance to organizations on how to mitigate NTLM relay attacks by default, days after researchers reported finding a NTLM hash disclosure zero-day in all versions of Windows Workstation and Server, from Windows 7 to current Windows 11 versions. https://www.darkreading.com/application-security/microsoft-ntlm-zero-day-remain-unpatched-april
- ***Researchers Uncover Prompt Injection Vulnerabilities in DeepSeek and Claude AI –*** Details have emerged about a now-patched security flaw in the DeepSeek artificial intelligence (AI) chatbot that, if successfully exploited, could permit a bad actor to take control of a victim's account by means of a prompt injection attack. https://thehackernews.com/2024/12/researchers-uncover-prompt-injection.html

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

ATTACKS, BREACHES & LEAKS

- ***Major Auto Parts Firm LKQ Hit by Cyberattack -*** LKQ Corporation, a major US-based provider of auto parts, informed the SEC late last week that a recent cyberattack caused disruptions at a Canadian business unit. https://www.securityweek.com/major-auto-parts-firm-lkq-hit-by-cyberattack/
- ***Sensitive Data Leaked After Namibia Ransomware Hack*** - Namibia's state-owned telecoms company has fallen victim to what is known as a ransomware attack resulting in the leak of sensitive customer data, including reportedly information about top government officials. https://databreaches.net/2024/12/17/sensitive-data-leaked-after-namibia-ransomware-hack/
- ***Certified Information Security Ransomware Breach by Bashe Group -*** Certified Information Security (CIS), a leader in corporate governance advisory services and training, has allegedly fallen victim to a ransomware attack claimed by the Bashe hacking group. This incident highlights the vulnerabilities even within organizations dedicated to cybersecurity education. https://www.halcyon.ai/attacks/certified-information-security-ransomware-breach-by-bashe-group
- ***Texas Tech University System data breach impacts 1.4 million patients*** - The Texas Tech University Health Sciences Center and its El Paso counterpart suffered a cyberattack that disrupted computer systems and applications, potentially exposing the data of 1.4 million patients. https://www.bleepingcomputer.com/news/security/texas-tech-university-system-data-breach-impacts-14-million-patients/
- ***Canadian Eyecare Firm Care1 Exposes 2.2TB of Patient Records*** - Cybersecurity researcher Jeremiah Fowler recently discovered a massive database belonging to Care1, a Canadian company that provides AI-powered software solutions to optometrists. The database, containing over 4.8 million records of patient information (with a total size of 2.2 TB), was left completely unprotected, exposing sensitive data like patient names, addresses, medical histories, and even their unique Personal Health Numbers (PHNs). https://hackread.com/canadian-eyecare-firm-care1-exposes-patient-records/

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. NUUO NVRmini –
    a. https://www.cve.org/CVERecord?id=CVE-2018-14933
    b. https://www.cve.org/CVERecord?id=CVE-2022-23227
2. Reolink –
    a. https://www.cve.org/CVERecord?id=CVE-2019-11001
    b. https://www.cve.org/CVERecord?id=CVE-2021-40407

SUSE Security Updates

1. Plymouth –
    a. https://www.suse.com/support/update/announcement/2024/suse-ru-20244373-1
    b. https://www.suse.com/support/update/announcement/2024/suse-ru-20244372-1
    c. https://www.suse.com/support/update/announcement/2024/suse-ru-20244371-1
    d. https://www.suse.com/support/update/announcement/2024/suse-ru-20244370-1
    e. https://www.suse.com/support/update/announcement/2024/suse-ru-20244369-1
2. Linux Kernel - https://www.suse.com/support/update/announcement/2024/suse-su-20244376-1
3. Publicsuffix - https://www.suse.com/support/update/announcement/2024/suse-ru-20244375-1

Check Point Security Advisories

1. OSGeo - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-0559.html
2. Cleo - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-1166.html
3. SolarWinds - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2015-1675.html
4. Atlassian - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2023-1486.html

Red Hat Security Advisories

1. gstreamer1-plugins-base and gstreamer1-plugins-good - https://access.redhat.com/errata/RHSA-2024:11344
2. gstreamer1-plugins-base - https://access.redhat.com/errata/RHSA-2024:11345
3. gstreamer1-plugins-good - https://access.redhat.com/errata/RHSA-2024:11346
4. Red Hat Advanced Cluster Management 2.11.4 - https://access.redhat.com/errata/RHSA-2024:11381

OTHER

1. Chrome –
    a. https://chromereleases.googleblog.com/2024/12/chrome-beta-for-ios-update_18.html
    b. https://chromereleases.googleblog.com/2024/12/chrome-beta-for-android-update_18.html