Information Sharing &
Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

# Daily Open-Source Cyber Report

December 11, 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**

- INTERPOL Arrests 5,500 in Global Cybercrime Crackdown, Seizes Over $400 Million
- Britain's Railways In Comms Meltdown
- Ransomware Gangs' Merciless Attacks Bleed Small Companies Dry
- Data Deletion Enters The Ransomware Chat
- How Attackers Use Corrupted Files to Slip Past Security
- The Shocking Speed Of Aws Key Exploitation
- How Threat Actors Can Use Generative Artificial Intelligence

**Emerging Threats & Vulnerabilities**

- I-O Data Confirms Zero-Day Attacks on Routers, Full Patches Pending
- New Rockstar 2FA Phishing-as-a-Service Kit Targets Microsoft 365 Accounts
- Venom Spider Spins Web of New Malware for MaaS Platform
- Veeam Warns Of Critical RCE Bug In Service Provider Console
- Hackers Use Corrupted ZIPs and Office Docs to Evade Antivirus and Email Defenses

**Attacks, Breaches, & Leaks**

- [NITROGEN] – Ransomware Victim: Mission Constructors , Inc[.]
- Rumpke Waste & Recycling Targeted In Apparent Cyber Attack
- Krispy Kreme Is Struggling To Fulfill Online Orders After It Was Hit With A Cyberattack
- Thousands of Social Security Numbers Stolen from New Jersey City Workers
- Deloitte Denied Its Systems Were Hacked By Brain Cipher Ransomware Group

# EXECUTIVE NEWS

**INTERPOL Arrests 5,500 in Global Cybercrime Crackdown, Seizes Over $400 Million**
*The Hacker News, 12/2/2024*

A global law enforcement operation has led to the arrest of more than 5,500 suspects involved in financial crimes and the seizure of more than $400 million in virtual assets and government-backed currencies. The coordinated exercise saw the participation of authorities from 40 countries, territories, and regions as part of the latest wave of Operation HAECHI-V, which took place between July and November 2024, INTERPOL said. "The effects of cyber-enabled crime can be devastating – people losing their life savings, businesses crippled, and trust in digital and financial systems undermined," INTERPOL Secretary General Valdecy Urquiza said in a statement. https://thehackernews.com/2024/12/interpol-arrests-5500-in-global.html

**Britain's Railways In Comms Meltdown**
*Rail Tech , 12/6/2024*

A major communications failure has paralysed much of the British railway network, leading to freight delays and commuter cancellations. Fears over digital interference are at an all-time high, prompting concerns over cyber security as the story leads the British media. Meanwhile, train drivers across Britain were puzzled by the silence on their cab comms. Signallers felt as bereft as mission controllers with all their screens showing "LOS" – Loss of Signal. Hamilton to Hounslow, we have a problem. This morning, the wireless comms system that puts signallers in touch with drivers, just wasn't. That's no joke and it's left the British rail network in meltdown. https://www.railtech.com/all/2024/12/06/britains-railways-in-comms-meltdown/?gdpr=deny&gdpr=accept

**Ransomware Gangs' Merciless Attacks Bleed Small Companies Dry**
*Claims Journal, 12/4/2024*

The black-and-white message flickering across computer screens sparked panic at Knights of Old, a 158-year-old U.K. delivery company: "If you're reading this, it means the internal infrastructure of your company is fully or partially dead." Knights' network for managing trucks was down. So was the system for booking payments. From 2,000 miles away, a criminal, Russia-linked hacking gang known as Akira had sabotaged the computers at Knights of Old and two related trucking companies. To force negotiations, the crooks in June 2023 had deployed malicious software that encrypted Knights' files and then threatened to publish online its confidential internal data.
https://www.claimsjournal.com/news/national/2024/12/06/327772.htm

**Data Deletion Enters The Ransomware Chat**
*CSO, 12/6/2024*

Ransomware remains one of the biggest cyber threats to companies today. In a survey by security provider Cohesity, 83% of respondents said they were affected by a ransomware attack in the first half of 2024. According to security experts, there is no relief in sight for 2025 either. But according to security provider G Data, an unsettling trend may be emerging: Newer hacker gangs are increasingly using ransomware to delete data instead of "just" encrypting it. "We are currently observing a new generation of hackers who have significantly less technical skills than known criminal groups," reports Tim Berghoff, security evangelist at G Data CyberDefense.
https://www.csoonline.com/article/3618139/data-deletion-enters-the-ransomware-chat.html

**How Attackers Use Corrupted Files to Slip Past Security**
*Hack Read, 11/27/2024*

A new zero-day attack campaign has surfaced, leveraging corrupted files to slip past even the strongest security protection. Recently identified by cybersecurity researchers at ANY.RUN, this attack demonstrates how sophisticated modern cyber threats have become. By bypassing antivirus software, sandbox environments, and email spam filters, these malicious files reach their targets with alarming efficiency. Let's dive deeper into the details of this attack, explore why it's so effective, and uncover how it can be identified to prevent further damage. https://hackread.com/how-attackers-use-corrupted-files-slip-past-security/

**The Shocking Speed Of Aws Key Exploitation**
*Help Net Security, 12/2/2024*

It's no secret that developers often inadvertently expose AWS access keys online and we know that these keys are being scraped and misused by attackers before organizations get a chance to revoke them. The results of this test revealed that attackers tend to find and exploit (within a few minutes) AWS access keys leaked on GitHub and DockerHub, and within several hours those exposed on PyPI, Pastebin, and the Postman Community. AWS secrets published on GitLab, Crates.io, public GitHub Gists, JSFiddle, Stack Overflow, Reddit and Quora were exploited in 1 to 5 days. Only the keys revealed on npm and Private GitHub Gists remained unused. https://www.helpnetsecurity.com/2024/12/02/revoke-exposed-aws-keys/

**How Threat Actors Can Use Generative Artificial Intelligence**
*Hack Read, 12/2/2024*

The capabilities that make Generative Artificial Intelligence a powerful tool for progress also make it a significant threat in the cyber domain. The use of GAI by malicious actors is becoming increasingly common, enabling them to conduct a wide range of cyberattacks. From generating deepfakes to enhancing phishing campaigns, GAI is evolving into a tool for large-scale cyber offenses. GAI has captured the attention of researchers and investors for its transformative potential across industries. Unfortunately, its misuse by malicious actors is altering the cyber threat landscape. Among the most concerning applications of Generative Artificial Intelligence are the creation of deepfakes and disinformation campaigns, which are already proving to be effective and dangerous.
https://securityaffairs.com/171582/uncategorized/how-threat-actors-can-use-generative-artificial-intelligence.html

# TECHNICAL SUMMARY

## EMERGING THREATS & EXPLOITS

- ***I-O Data Confirms Zero-Day Attacks on Routers, Full Patches Pending -*** Japanese device maker I-O Data this week confirmed zero-day exploitation of critical flaws in multiple routers and warned that full patches won't be available for a few weeks. https://www.securityweek.com/i-o-data-confirms-zero-day-attacks-on-routers-full-patches-pending/
- ***New Rockstar 2FA Phishing-as-a-Service Kit Targets Microsoft 365 Accounts*** - Cybersecurity researchers at Trustwave have discovered "Rockstar 2FA," a phishing-as-a-service platform designed to help hackers and script kiddies bypass two-factor authentication (2FA) and gain unauthorized access to Microsoft 365 accounts. https://hackread.com/rockstar-2fa-phishing-as-a-service-microsoft-365-accounts/
- ***Venom Spider Spins Web of New Malware for MaaS Platform –*** A known threat actor in the malware-as-a-service (MaaS) business known as "Venom Spider" continues to expand capabilities for cybercriminals who use its platform, with a novel backdoor and loader detected in two separate attacks in a recent two-month period. https://www.darkreading.com/cyberattacks-data-breaches/venom-spider-malware-maas-platform
- ***Veeam Warns Of Critical RCE Bug In Service Provider Console –*** Veeam released security updates today to address two Service Provider Console (VSPC) vulnerabilities, including a critical remote code execution (RCE) discovered during internal testing. https://www.bleepingcomputer.com/news/security/veeam-warns-of-critical-rce-bug-in-service-provider-console/
- ***Hackers Use Corrupted ZIPs and Office Docs to Evade Antivirus and Email Defenses -*** Cybersecurity researchers have called attention to a novel phishing campaign that leverages corrupted Microsoft Office documents and ZIP archives as a way to bypass email defenses. https://thehackernews.com/2024/12/hackers-use-corrupted-zips-and-office.html

## ATTACKS, BREACHES & LEAKS

- ***[NITROGEN] – Ransomware Victim: Mission Constructors , Inc[.] -*** The ransomware leak page focuses on Mission Constructors, Inc., a construction management company based in Houston, Texas. The company specializes in various services, including design/build, value engineering, and comprehensive construction services across the state of Texas. https://www.redpacketsecurity.com/nitrogen-ransomware-victim-mission-constructors-inc/
- ***Rumpke Waste & Recycling Targeted In Apparent Cyber Attack*** - Current and former employees at Rumpke Waste & Recycling may have had their personal information compromised after an apparent cyber attack this summer, the company said on Dec. 10. https://www.wave3.com/2024/12/10/rumpke-waste-recycling-targeted-apparent-cyber-attack/
- ***Krispy Kreme Is Struggling To Fulfill Online Orders After It Was Hit With A Cyberattack -*** A cybersecurity attack is hampering some customers from getting their doughnuts at Krispy Kreme, the company revealed Wednesday. The chain said in a regulatory statement that it had detected "unauthorized activity on a portion" of its technology late last month that is still causing "certain operational disruptions," notably its online ordering function for portions of the United States. https://www.cnn.com/2024/12/11/business/krispy-kreme-cyber-attack-hack/index.html
- ***Thousands of Social Security Numbers Stolen from New Jersey City Workers*** - The social security numbers, driver's licenses, payroll, health and other personal details of Hoboken city workers were among the data stolen in a "massive" cybersecurity breach last month. https://www.governing.com/workforce/thousands-of-social-security-numbers-stolen-from-new-jersey-city-workers
- ***Deloitte Denied Its Systems Were Hacked By Brain Cipher Ransomware Group*** - Recently, the ransomware group Brain Cipher added Deloitte UK to its Tor leak site. The gang claimed to have stolen one terabyte of compressed data from the company. https://securityaffairs.com/171827/uncategorized/deloitte-denied-its-systems-were-hacked-by-brain-cipher-ransomware-group.html

## SECURITY VULNERABILITIES, ALERTS, ADVISORIES, & UPDATES

### SUSE Security Updates

1. Curl –
   a. https://www.suse.com/support/update/announcement/2024/suse-su-20244287-1
   b. https://www.suse.com/support/update/announcement/2024/suse-su-20244288-1
2. python-rpm-macros - https://www.suse.com/support/update/announcement/2024/suse-ru-20244289-1
3. libsoup2 - https://www.suse.com/support/update/announcement/2024/suse-su-20244290-1
4. python312 - https://www.suse.com/support/update/announcement/2024/suse-su-20244291-1
5. webkit2gtk3 - https://www.suse.com/support/update/announcement/2024/suse-su-20244292-1
6. socat - https://www.suse.com/support/update/announcement/2024/suse-su-20244294-1

### Gentoo Security Advisories

1. Dnsmasq - https://security.gentoo.org/glsa/202412-10
2. Salt - https://security.gentoo.org/glsa/202412-09
3. icinga2 - https://security.gentoo.org/glsa/202412-08
4. OpenJDK - https://security.gentoo.org/glsa/202412-07
5. Asterisk - https://security.gentoo.org/glsa/202412-03

### Fedora Security Advisories

1. python3.14 - https://lwn.net/Articles/1001705

### Debian Security Advisories

1. proftpd-dfsg - https://lists.debian.org/debian-security-announce/2024/msg00243.html
2. smarty3 - https://lists.debian.org/debian-security-announce/2024/msg00242.html

### Check Point Security Advisories

1. Apache - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-1150.html
2. Microsoft – https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-1114.html
3. Progress - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-1149.html
4. Ivanti - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-1062.html

**SENSITIVE & PROPRIETARY INFROMATION - NOT FOR PUBLIC DISSEMINATION**

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

### Drupal Security Advisories

1. Entity Form Steps - https://www.drupal.org/sa-contrib-2024-071
2. Minify JS - https://www.drupal.org/sa-contrib-2024-070
3. Download All Files - https://www.drupal.org/sa-contrib-2024-069
4. Pages Restriction Access - https://www.drupal.org/sa-contrib-2024-068
5. OAuth & OpenID Connect Single Sign On - https://www.drupal.org/sa-contrib-2024-067
6. Print Anything - https://www.drupal.org/sa-contrib-2024-066
7. Megamenu Framework - https://www.drupal.org/sa-contrib-2024-065

### Red Hat Security Advisories

1. php:8.2 - https://access.redhat.com/errata/RHSA-2024:10949
2. php:8.1 - https://access.redhat.com/errata/RHSA-2024:10950
3. python36:3.6 - https://access.redhat.com/errata/RHSA-2024:10953
4. ruby - https://access.redhat.com/errata/RHSA-2024:10961

### Ubuntu Security Notices

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

### Zero Day Initiative Advisories & Updates

1. GFI Archiver –
   a. https://www.zerodayinitiative.com/advisories/ZDI-24-1672/
   b. https://www.zerodayinitiative.com/advisories/ZDI-24-1671/
   c. https://www.zerodayinitiative.com/advisories/ZDI-24-1670/
2. Veritas -
   a. https://www.zerodayinitiative.com/advisories/ZDI-24-1669/
   b. https://www.zerodayinitiative.com/advisories/ZDI-24-1668/
   c. https://www.zerodayinitiative.com/advisories/ZDI-24-1667/

## OTHER

- Google –
  - https://chromereleases.googleblog.com/2024/12/extended-stable-updates-for-desktop_10.html
  - https://chromereleases.googleblog.com/2024/12/stable-channel-update-for-desktop_10.html
  - https://chromereleases.googleblog.com/2024/12/chrome-stable-for-ios-update_95.html
  - https://chromereleases.googleblog.com/2024/12/chrome-beta-for-desktop-update.html

### *** FAIR USE NOTICE***

This message contains copyrighted material whose use has not been specifically authorized by the copyright owner. The ST-ISAC is making it available to ISAC members who have expressed a prior interest in receiving information to advance their understanding of threat activities in the interest of protecting the national infrastructure of the United States.  We believe that this constitutes a 'fair use' of the copyrighted material as provided for in section 107 of the U.S. Copyright Law. If you wish to use this copyrighted material for purposes of your own that go beyond 'fair use,' you must obtain permission from the copyright owner.