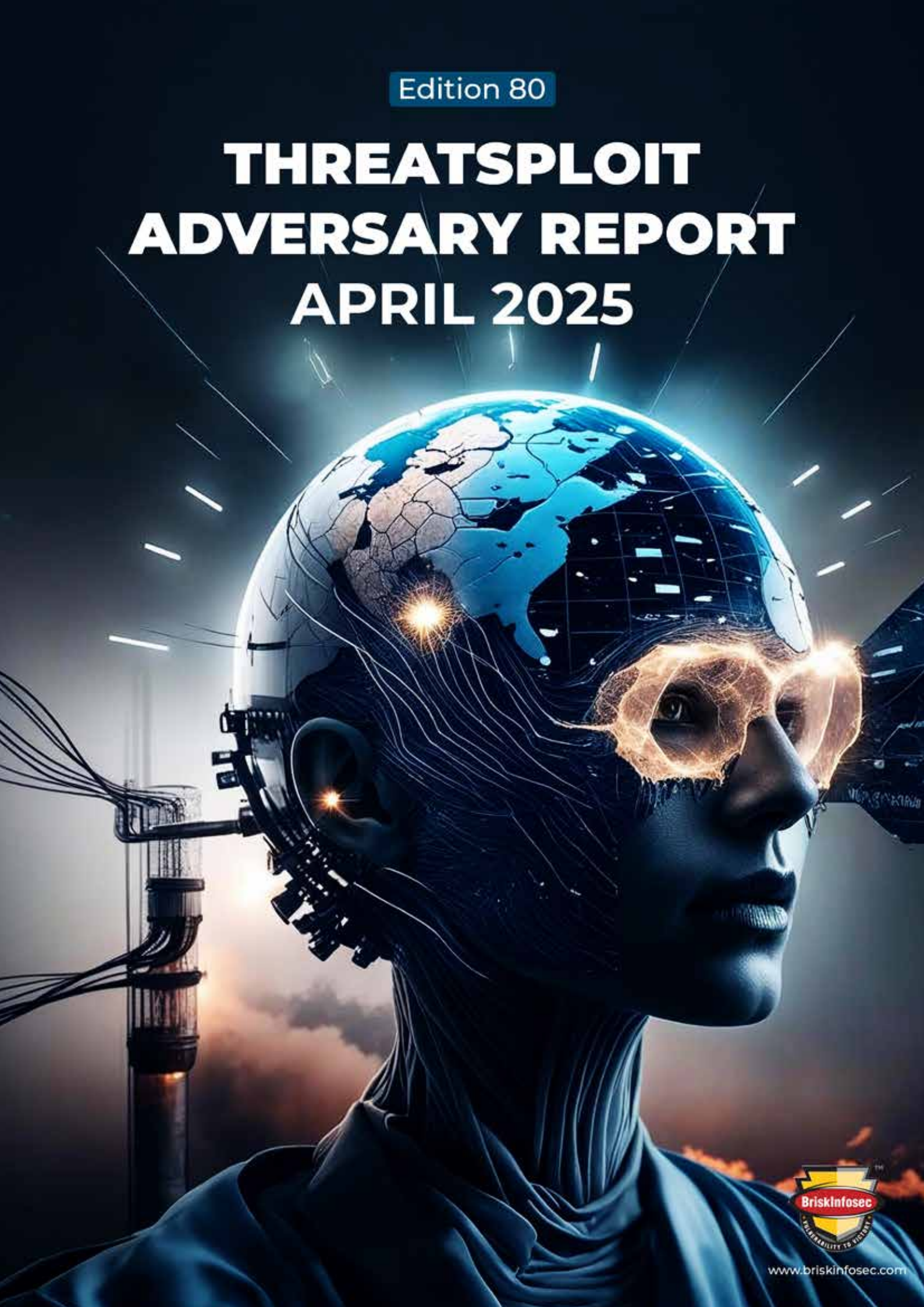
Edition 80

THREATSPLOIT ADVERSARY REPORT APRIL 2025



BriskInfosec

www.briskinfosec.com

Introduction

Dear Readers

Cybercrime never sleeps, and neither do we. The April 2025 Threatsploit Adversary Report is here, breaking down the 30 most shocking cyberattacks that shook industries this month. From high-profile data breaches to sophisticated ransomware takedowns, hackers are finding new ways to stay ahead. Organizations must continuously adapt to keep pace with these evolving threats.

This month, ransomware attacks surged, exploiting unpatched vulnerabilities and weak cloud configurations. A global enterprise faced a devastating breach, exposing millions of sensitive records. Healthcare systems suffered a supply chain attack, crippling operations. Financial institutions were hit hard by phishing scams that bypassed multi-factor authentication, leading to massive fraud. Meanwhile, state-backed hackers launched stealthy intrusions into government networks, showcasing the next level of cyber espionage.

With AI-powered malware, deepfake-driven scams, and API vulnerabilities in play, traditional security methods are falling short. The modern attacker doesn't just break in, they blend in. Organizations must rethink their cybersecurity strategies with zero-trust frameworks, real-time threat intelligence, and smarter incident response plans to strengthen their defenses.

Staying ahead of cybercriminals requires vigilance, adaptability, and intelligence. The Threatsploit Adversary Report delivers actionable insights to help security teams anticipate threats before they escalate, ensuring organizations remain resilient in the face of evolving cyber risks.

Best Regards,

Briskinfosec Threat Intelligence Team

Contents :

Blind Eagle APT Targets Colombian Institutions with Sophisticated Spear-Phishing and Malware Campaigns

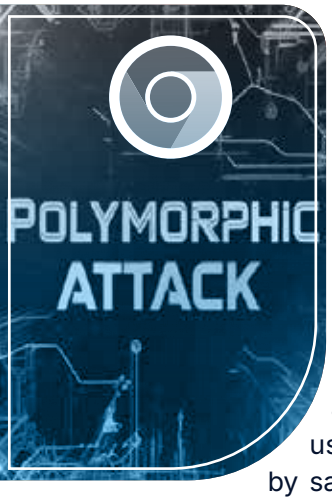
Blind Eagle, an APT group active since at least 2018, has been targeting Colombian institutions and government entities since November 2024. The group uses spear-phishing emails and social engineering to deliver remote access trojans (RATs) such as AsyncRAT, NjRAT, Quasar RAT, and Remcos RAT. Recent attacks stand out for exploiting the newly patched Windows vulnerability CVE-2024-43451, which allows the group to trigger infections even before the victim interacts with the malicious file. They also use HeartCrypt, a packer-as-a-service, to protect the payload and evade detection.

The group has expanded its malware distribution beyond Google Drive and Dropbox, now using GitHub and Bitbucket. In a mistake, Blind Eagle exposed sensitive data, including 1,634 email accounts, passwords, and ATM PINs, on a GitHub repository. The group's success is due to its ability to exploit legitimate file-sharing platforms, advanced evasion techniques, and connections to the cybercriminal ecosystem.

Attack Type : Spear-phishing

Cause of Issue : Exploited Vulnerabilities

Industry : Government Sector



Polymorphic Extension Attack Targets Chromium Browsers to Steal User Credentials

Researchers have identified a new cyberattack method using polymorphic browser extensions that can impersonate legitimate ones in Chromium-based browsers like Google Chrome, Microsoft Edge, and Brave. The attack involves a rogue extension mimicking the target extension's icon, HTML popup, and workflows while temporarily disabling the real extension through the chrome management API. The malicious extension initially appears as a harmless utility but then scans for specific installed extensions using a technique called web resource hitting. Once a target extension is found, the rogue extension morphs to replicate it and harvests credentials when users interact with it, potentially giving attackers unauthorized access to personal and financial information. The attack exploits users' reliance on visual cues, particularly the icons of pinned extensions. Google responded by saying they are constantly improving security on the Chrome Web Store and taking action against emerging threats.

Attack Type : Extension Impersonation

Cause of Issue : Extension Manipulation

Industry : Information Technology

Malicious Cobalt Strike Campaign Targeting Japan's Sectors

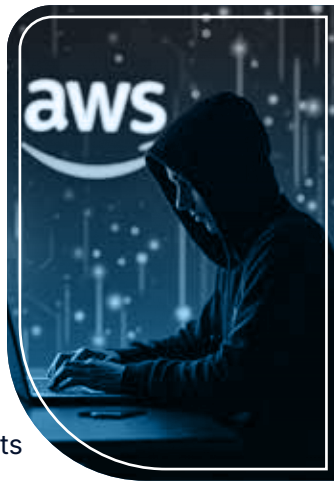
A malicious campaign, attributed to unknown threat actors, has been targeting organizations in Japan since January 2025. The attackers exploit the CVE-2024-4577 vulnerability in PHP-CGI on Windows to gain initial access and deploy a Cobalt Strike reverse HTTP shellcode for persistent remote access. Following this, they conduct reconnaissance, privilege escalation, and lateral movement using various tools, including JuicyPotato and Mimikatz, to exfiltrate passwords and NTLM hashes. The attackers maintain stealth by erasing event logs and modifying system settings for persistence. The Cobalt Strike tools, hosted on Alibaba cloud servers, expose additional adversarial frameworks, such as BeEF, Viper C2, and Blue-Lotus, which enable further exploitation and attacks. The campaign primarily targets sectors like technology, telecommunications, entertainment, education, and e-commerce. The attackers' activities suggest a broader goal beyond credential harvesting, indicating potential future attacks.

Attack Type : Remote Exploitation

Cause of Issue : PHP Vulnerability

Industry : Telecommunication

Threat Actor Group Exploits AWS Misconfigurations for Phishing Campaigns



Palo Alto Networks' Unit 42 has tracked a threat actor group, TGR-UNK-0011 (also linked to JavaGhost), targeting Amazon Web Services (AWS) environments to carry out phishing campaigns. The group, active since 2019, initially focused on defacing websites but shifted to phishing for financial gain in 2022. They exploit misconfigurations in AWS environments, such as exposed access keys, to use Amazon Simple Email Service (SES) and WorkMail for phishing emails. This tactic avoids email protection systems since the messages appear to come from a legitimate source. The group has evolved its techniques, including obfuscating their identity in CloudTrail logs and creating unused IAM users for long-term access. They also establish persistence through new IAM roles, trust policies, and security groups named "Java_Ghost." These actions allow them to maintain control over compromised AWS accounts without being easily detected.

Attack Type : Phishing Campaign | Cause of Issue : AWS Misconfigurations | Industry : SaaS Providers

Zero-Day Vulnerabilities in Paragon Partition Manager Driver Exploited for Ransomware Attacks

Threat actors are exploiting a zero-day vulnerability (CVE-2025-0289) in the BioNTdrv.sys driver of Paragon Partition Manager to escalate privileges and execute arbitrary code in ransomware attacks. Discovered by Microsoft and affecting BioNTdrv.sys versions 1.3.0 and 1.5.1, this vulnerability is part of a set of five flaws that include arbitrary kernel memory mapping, write vulnerabilities, and null pointer dereference. These vulnerabilities allow attackers with local access to escalate privileges or trigger a denial-of-service (DoS) condition. The flaws can also facilitate Bring Your Own Vulnerable Driver (BYOVD) attacks, enabling adversaries to gain elevated privileges and execute malicious code on unpatched systems. Paragon Software has addressed the vulnerabilities in version 2.0.0 of the driver, and Microsoft has added the affected driver version to its blocklist. This discovery follows a recent malware campaign exploiting another vulnerable Windows driver to deploy Ghost RAT malware.

Attack Type : Privilege Escalation | Cause of Issue : Vulnerable Driver | Industry : Software development

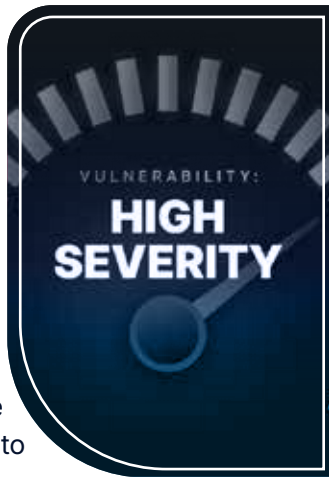
Medusa Ransomware Targets 40+ Victims in 2025, Ransoms Range from $100K to $15M

Medusa ransomware, operated by the Spearwing group, has claimed nearly 400 victims since its emergence in January 2023, with a 42% increase in attacks from 2023 to 2024. In early 2025, over 40 attacks were reported. The group uses double extortion tactics, stealing data before encrypting systems and threatening to publish it if ransoms aren't paid. Medusa has targeted various sectors, including healthcare, finance, and government, demanding ransoms between $100,000 and $15 million. Attackers exploit security flaws in public-facing applications, particularly Microsoft Exchange Server, and use tools like SimpleHelp, AnyDesk, and MeshAgent for persistent access. They also deploy KillAV to disable antivirus processes and use PDQ Deploy for lateral movement across networks. Medusa's rise coincides with a shift in the ransomware landscape, as groups like LockBit and BlackCat have seen disruptions, creating opportunities for newer players like Medusa to thrive.

Attack Type : Ransomware Attack | Cause of Issue : Security Flaw

Industry : Healthcare

High-Severity Vulnerability in FreeType Library Exposes Linux Systems to Remote Code Execution



Meta has warned of a high-severity security vulnerability in the FreeType open-source font rendering library, identified as CVE-2025-27363, with a CVSS score of 8.1. The flaw, an out-of-bounds write, affects FreeType versions 2.13.0 and below, and could allow remote code execution when parsing certain font files. The vulnerability arises from a code error where a signed short value is assigned to an unsigned long, causing heap buffer overflows and potential arbitrary code execution. While Meta didn't provide specifics on exploitation details, it acknowledged the flaw may have been actively exploited. FreeType developer Werner Lemberg confirmed that a fix has been available for nearly two years in versions newer than 2.13.0. Several Linux distributions, including AlmaLinux, Ubuntu, and Debian, are still running outdated, vulnerable versions, leaving users at risk. It's advised to update to FreeType version 2.13.3 for protection.

Attack Type : Remote code execution

Cause of Issue : Out-of-bounds write

Industry : Software development

Cybercriminals Use CSS to Bypass Spam Filters and Monitor Email User Activity

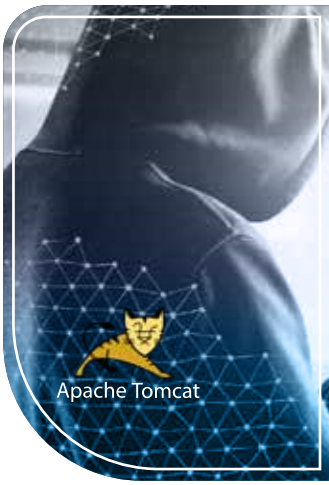
Malicious actors are exploiting CSS (Cascading Style Sheets) to bypass spam filters and track users' actions, according to Cisco Talos. By leveraging CSS properties like text-indent and opacity, attackers can hide content in emails, evading detection while potentially redirecting victims to phishing sites. CSS also enables tracking of user behavior, such as identifying font preferences, language, and even actions like viewing or printing emails. The @media CSS at-rule can detect screen size, resolution, and color depth, aiding in user fingerprinting. This abuse compromises user privacy and security, particularly in email clients that restrict dynamic content like JavaScript. To mitigate risks, advanced filtering mechanisms and email privacy proxies are recommended to detect hidden text and concealment tactics.

Attack Type : CSS Exploitation

Cause of Issue : Content Concealment

Industry : Information Technology

Critical Apache Tomcat Vulnerability Exploited for Remote Code Execution



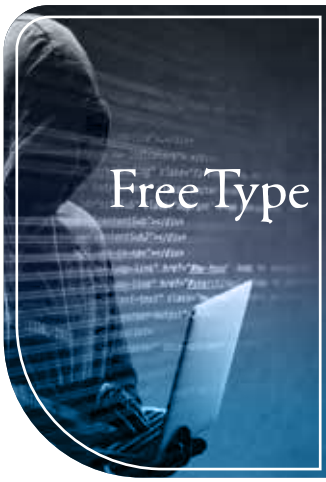
A recently disclosed vulnerability in Apache Tomcat, tracked as CVE-2025-24813, is being actively exploited in the wild. The flaw affects Tomcat versions 9.0.0-M1 to 11.0.2 and could lead to remote code execution or information disclosure under specific conditions. The vulnerability allows attackers to exploit Tomcat's default servlet and partial PUT support to upload malicious files, potentially leading to the injection of arbitrary content or remote code execution. The exploit leverages Tomcat's file-based session persistence and deserialization of a malicious Java session file. The vulnerability is easy to exploit and does not require authentication, with attackers able to upload malicious JSP files and modify configurations. Apache Tomcat has released patches in versions 9.0.99, 10.1.35, and 11.0.3. Users are advised to update their instances promptly to avoid risks of exploitation.

Attack Type : Remote Code Execution

Cause of Issue : Partial PUT

Industry : Information Technology

Critical Vulnerability in FreeType Library Exposes Systems to Remote Code Execution



Meta has issued a warning about a high-severity security vulnerability (CVE-2025-27363) in the FreeType open-source font rendering library, affecting versions 2.13.0 and below. The flaw, described as an out-of-bounds write, can lead to remote code execution when parsing certain font files, specifically related to TrueType GX and variable font files. The issue arises from a signed short value being assigned to an unsigned long, causing a heap buffer to be allocated too small, potentially allowing arbitrary code execution. While the vulnerability has been patched in FreeType versions above 2.13.0, several Linux distributions, including AlmaLinux, Alpine Linux, Debian, RHEL, Ubuntu, and others, are running outdated versions, making them susceptible to exploitation. Meta has acknowledged that the bug may have been exploited in the wild, urging users to update to FreeType version 2.13.3 for protection.

Attack Type : Remote code execution

Cause of Issue : Out-of-bounds write

Industry : Software development

Hackers Leverage Critical PHP Vulnerability to Deploy Quasar RAT and Cryptomining Malware

A severe vulnerability in PHP, identified as CVE-2024-4577, affects Windows systems running in CGI mode, allowing remote attackers to execute arbitrary code. This flaw has been exploited to deliver cryptocurrency miners like XMRig and Nicehash, and remote access tools such as Quasar RAT. Bitdefender has observed a significant increase in exploitation attempts since late 2023, especially in Taiwan, Hong Kong, and Brazil. Attacks typically involve basic vulnerability checks, system reconnaissance, and malicious payloads. In some cases, attackers modify firewall configurations to block rival cryptojacking groups from accessing compromised servers. This unusual tactic suggests competition among cybercriminals. To mitigate the risk, users are advised to update PHP to the latest version and limit the use of tools like PowerShell to privileged users.

Attack Type : Cryptojacking

Cause of Issue : PHP Vulnerability

Industry : Information Technology

SSRF Vulnerability in Third-Party ChatGPT Tool Targets Financial and Government Sectors

A year-old server-side request forgery (SSRF) vulnerability, CVE-2024-27564, is being actively exploited by threat actors targeting financial and government organizations. The vulnerability, found in a third-party ChatGPT tool developed by a Chinese creator, allows attackers to inject malicious URLs through the pictureproxy.php file, triggering arbitrary requests. Discovered in September 2023 and publicly disclosed a year ago, it is exploitable without authentication. Cybersecurity firm Veriti reported over 10,000 attack attempts from a single IP address in one week, with many organizations in the US, Germany, and other countries at risk due to misconfigurations in security systems. Financial, healthcare, and government entities, particularly in AI-driven sectors, are prime targets, as SSRF attacks can access internal resources or steal sensitive data. Organizations are urged to patch the vulnerability, check firewalls and intrusion prevention systems, and monitor logs for known attacker IPs.

Attack Type : SSRF Attack

Cause of Issue : Vulnerable in Third-party Tool

Industry : Financial Sector

New DLL Side-Loading Attack Exploits Vulnerability in Google Chrome 133

A vulnerability in Google Chrome version 133.0.6943.126 allows attackers to exploit DLL side-loading techniques, enabling malicious code execution through Chrome's trusted subprocesses. The attack occurs when attackers replace the legitimate chrome_elf.dll file with a malicious one, taking advantage of Windows' search order for DLLs. The malicious DLL loads during Chrome's operation, executing code with the browser's trusted permissions. This sophisticated attack also employs DLL proxying, where the malicious DLL intercepts and forwards function calls to the legitimate one, maintaining normal browser behavior while executing harmful actions. The attack uses the Nim programming language to evade detection, and security tools have identified the malicious DLL in only 2 out of 70 scans. Users are urged to update Chrome immediately and deploy endpoint detection solutions to mitigate the risk, as this vulnerability remains exploitable despite other fixes in Chrome 133.

Attack Type : DLL Side-Loading | Cause of Issue : Malicious DLL | Industry : Information Technology

State-Backed Hackers Exploit Windows Vulnerability in Ongoing Espionage and Data Theft Campaigns

A Windows vulnerability, tracked as ZDI-CAN-25373, has been exploited in cyber espionage and data theft attacks by at least 11 state-backed hacking groups, including North Korea, Iran, Russia, and China, since 2017. This flaw, caused by a User Interface Misrepresentation in shortcut (.lnk) files, allows attackers to hide malicious command-line arguments using padded whitespaces, making the code undetectable to users. Once a user interacts with a malicious file or webpage, the attacker can execute arbitrary code. Although Microsoft has yet to release a patch, the vulnerability has been actively exploited with various malware payloads, including Ursnif and Trickbot, targeting North America, South America, Europe, and East Asia. Trend Micro researchers discovered nearly 1,000 exploitation samples and warned that many more attempts likely exist. Microsoft has acknowledged the issue and may address it in a future update, recommending caution with downloading files from untrusted sources.

Attack Type : Cyber Espionage | Cause of Issue : UI Misrepresentation | Industry : Financial Sector

Apache Tomcat RCE Vulnerability Targeted by 2-Step Exploit

A critical remote code execution (RCE) vulnerability in Apache Tomcat, tracked as CVE-2025-24813, is being actively exploited in the wild. The exploit allows attackers to take control of servers via a two-step process: first, they upload a malicious Java session file through a PUT request, then trigger deserialization by referencing the session ID in a GET request. Discovered in March 2025, the attack bypasses most Web Application Firewalls (WAFs) because the PUT request appears normal, the payload is base64-encoded, and the harmful action occurs only at the end of the attack. With no authentication required and file-based session storage being common, this vulnerability is relatively easy to exploit. Red Hat rated it a moderate 8.6 out of 10 in severity. Experts recommend implementing real-time API security to decode payloads, analyze requests deeply, and block multi-step attacks to protect against evolving threats.

Attack Type : Remote Code Execution | Cause of Issue : Session Deserialization | Industry : Information Technology

Over 20,000 WordPress Sites Targeted in DollyWay Malware Attack

The DollyWay malware operation has compromised over 20,000 WordPress sites since 2016, redirecting visitors to scam sites using advanced evasion and reinfection tactics. In its latest version (v3), DollyWay generates 10 million fraudulent impressions per month by redirecting traffic through a Traffic Direction System (TDS) to monetize via VexTrio and LosPollos affiliate networks. It exploits n-day vulnerabilities in WordPress plugins and themes, injecting malicious scripts and hiding itself by creating hidden admin accounts and modifying WPCode. Its auto-reinfection mechanism makes it hard to remove, as it spreads across all active plugins and reloads with every page visit.

Attack Type : Malvertising attack

Cause of Issue : Plugin vulnerabilities

Industry : E-commerce

Data Breach at Pennsylvania Education Union Affects 500,000 Individuals

The Pennsylvania State Education Association (PSEA) experienced a data breach in July 2024, affecting 517,487 individuals. Stolen data includes personal, financial, and health information such as Social Security numbers, driver's licenses, and payment details. The Rhysida ransomware gang claimed responsibility, demanding a 20 BTC ransom. PSEA is offering free credit monitoring to affected individuals and advising them to monitor their financial activity. Rhysida has been linked to several high-profile attacks, including on the British Library, Insomniac Games, and Lurie Children's Hospital.

Attack Type : Ransomware attack

Cause of Issue : Data breach

Industry : Education

WhatsApp Fixes Zero-Click Vulnerability Used in Paragon Spyware Campaigns

WhatsApp patched a zero-click, zero-day vulnerability exploited by Paragon's Graphite spyware to target journalists and activists. The attack involved sending a malicious PDF via WhatsApp, which automatically installed the spyware to access private communications and compromise other apps. WhatsApp notified around 90 affected Android users in over two dozen countries. Citizen Lab linked the spyware's infrastructure to Paragon and multiple government customers, including in Israel, Australia, and Canada. Paragon, founded by former Israeli leaders and acquired by AE Industrial Partners in 2024, claims it only sells its tools to democratic law enforcement agencies.

Attack Type : Spyware attack

Cause of Issue : Zero-click vulnerability

Industry : Software development company

Western Alliance Bank Informs 21,899 Customers of Data Breach

Western Alliance Bank notified nearly 22,000 customers that their personal data, including Social Security numbers, financial details, and IDs, was stolen in an October 2024 breach. The attack exploited a zero-day vulnerability in Cleo's secure file transfer software, which was targeted by the Clop ransomware gang. The breach affected Western Alliance and 57 other companies. The stolen data was only discovered after it was leaked online. The bank is offering free credit monitoring and identity protection services to the affected customers.

Attack Type : Ransomware attack

Cause of Issue : Zero-day vulnerability

Industry : Financial and banking

Critical PHP Vulnerability Used to Deploy Quasar RAT and XMRig Miners

A severe security vulnerability in PHP, tracked as CVE-2024-4577, is being actively exploited by threat actors to deploy cryptocurrency miners like XMRig and remote access trojans (RATs) such as Quasar RAT. The flaw, affecting Windows systems running PHP in CGI mode, allows remote attackers to execute arbitrary code. Exploitation attempts have been observed globally, with significant activity in Taiwan, Hong Kong, Brazil, Japan, and India. The attacks involve system reconnaissance and the deployment of mining software, disguised as legitimate programs. Cybersecurity experts recommend updating PHP installations and limiting the use of tools like PowerShell to prevent exploitation.

Attack Type : Cryptojacking | Cause of Issue : PHP vulnerability | Industry : Information Technology

Severe PHP Vulnerability Used to Deploy Quasar RAT and Cryptocurrency Miners

A severe PHP vulnerability (CVE-2024-4577) affecting Windows systems in CGI mode is being exploited by attackers to deploy cryptocurrency miners like XMRig and remote access trojans (RATs) such as Quasar RAT. The flaw allows remote code execution and has led to a surge in exploitation attempts, with major concentrations in Taiwan, Hong Kong, and Brazil. Exploited vulnerabilities also lead to system reconnaissance, miner deployment, and firewall modifications. Organizations are advised to update their PHP installations and restrict the use of tools like PowerShell to prevent further exploitation.

Attack Type : Cryptojacking | Cause of Issue : PHP vulnerability | Industry : Information Technology

Coinbase First Targeted in GitHub Actions Supply Chain Attack; 218 Repositories Expose CI/CD Secrets

A supply chain attack involving the GitHub Action "tj-actions/changed-files" was initially targeted at Coinbase's open-source project but later expanded to affect 218 repositories. The attacker exploited vulnerabilities in GitHub Actions to inject malicious code that leaked sensitive secrets, including credentials for DockerHub, AWS, and npm. This attack leveraged compromised GitHub tokens and affected both Coinbase's and other repositories that relied on the action. The attacker used advanced tactics, including creating fake accounts and obfuscating actions, likely aiming for financial gain through cryptocurrency theft. The breach was discovered on March 14, 2025, and GitHub is reviewing the situation.

Attack Type : Supply Chain | Cause of Issue : Code Injection | Industry : Software development Industry

China's Aquatic Panda APT Launches 10-Month Espionage Campaign, Targets 7 Global Entities with 5 Malware Families

The China-linked APT group, Aquatic Panda, carried out a global espionage campaign, Operation FishMedley, between January and October 2022. Targeting seven organizations, including governments, NGOs, and think tanks in Taiwan, Hungary, Turkey, Thailand, France, and the U.S., the group used malware like ShadowPad, SodaMaster, and Spyder. The attack, attributed to the Winnti Group, involved five different malware families and exploited various implants to gather intelligence. The full details of the attack's initial access vector are still unknown.

Attack Type : Cyber Espionage

Cause of Issue :Malware implants

Industry : Government sector

Critical Flaws in mySCADA myPRO Expose Industrial Systems to Potential Takeover

Cybersecurity researchers revealed two critical command injection vulnerabilities in mySCADA myPRO, a SCADA system used in industrial environments. Exploiting these flaws could allow attackers to execute arbitrary commands, potentially leading to severe operational disruptions and financial losses. The issues stem from improper input sanitization, and patched versions have been released. Organizations are advised to apply patches, enforce network segmentation, and monitor for suspicious activity.

Attack Type : Command injection

Cause of Issue : Input sanitization

Industry : Industrial control systems (ICS)

RansomHub Ransomware Deploys New Betruger Multi-Function Backdoor

Symantec researchers identified a custom backdoor called Betruger, used in recent ransomware attacks linked to the RansomHub RaaS operation. This multi-functional malware includes features like keylogging, network scanning, and credential dumping, and is designed to minimize the deployment of additional tools during attacks. Betruger is delivered using filenames that disguise it as a legitimate mailing app. RansomHub has been involved in data-theft extortion and has breached high-profile victims, including healthcare and critical infrastructure sectors.

Attack Type : Ransomware attack

Cause of Issue : Betruger Backdoor Exploitation

Industry : Healthcare

Malicious VSCode Extensions Discovered Distributing Early-Stage Ransomware

Two malicious extensions, "ahban.shiba" and "ahban.cychelloworld," were discovered on the VSCode Marketplace, deploying in-development ransomware. The extensions, which were downloaded a few times before being removed, contained a PowerShell script that downloaded ransomware from a remote server. The ransomware encrypted files in a specific test folder and displayed a ransom message. Despite being reported earlier, Microsoft took months to remove the extensions, revealing a gap in their review process. The extensions were accepted into the store after adding malicious code in subsequent versions.

Attack Type : Ransomware attack

Cause of Issue : Inadequate review

Industry : Software development industry

Oracle Disputes Hacker's Claim of Stealing 6 Million Data Records

Oracle has denied a breach after a threat actor, rose87168, claimed to have stolen 6 million records from Oracle Cloud's SSO servers. The attacker released files containing encrypted passwords, Java Keystore files, and other sensitive data, and is selling the information on BreachForums. Oracle stated that no customer data was affected and that the credentials are not linked to Oracle Cloud. The hacker alleges they accessed Oracle Cloud servers via a vulnerability in a public CVE, but Oracle has not confirmed this. The hacker also sought a ransom from Oracle but was reportedly refused.

Attack Type : Data exfiltration

Cause of Issue : Vulnerability exploitation

Industry : SaaS Providers

SANS Institute Alerts on Emerging Cloud-Native Ransomware Threats

A recent Palo Alto Networks Unit 42 report revealed that 66% of cloud storage buckets contain sensitive data, making them prime targets for ransomware attacks. The SANS Institute warns that attackers are abusing legitimate cloud security features, such as AWS S3 SSE-C and KMS external key material, to execute these attacks. To mitigate these risks, SANS advises organizations to understand the limitations of cloud security controls, as cloud storage is not inherently safe. They should also block unsupported encryption methods by enforcing IAM policies, enable backups, object versioning, and object locking for data recovery, and balance security with cost through carefully managed data lifecycle policies. However, organizations must remain cautious, as attackers can also exploit these policies. Proper cloud security measures are essential to protecting data from ransomware threats.

Attack Type : Ransomware attack

Cause of Issue : Cloud misconfigurations

Industry : SaaS Providers

Steam Removes Game Demo After Malware Infects Windows Systems

Phantom's Resolution from Steam after reports that its demo installer contained malware. The game, published by Sierra Six Studios, prompted users to download from an external GitHub repository, where malware disguised as Windows Defender SmartScreen.exe was found. The malware used privilege escalation tools, intercepted cookies, and added persistence via startup tasks. Reddit users uncovered suspicious elements, and GitHub quickly removed the repository. Valve later pulled the game, and the developer's website was taken offline. Users who installed it are advised to run a full system scan. This follows a similar incident last month with PirateFi, which spread the Vidar infostealer.

Attack Type : Malware infection

Cause of Issue : Malicious installer

Industry : Gaming Industry

Hackers Leverage Critical PHP Vulnerability to Install Quasar RAT and XMRig Miners

A China-aligned threat group, MirrorFace, launched a malware campaign targeting a Central European diplomatic organization in August 2024. Using spear-phishing lures related to the Word Expo, the group deployed a customized version of AsyncRAT and ANEL backdoor. The attack, part of Operation AkaiRyū, marks a shift from targeting Japanese entities to European ones. The group also used tactics like Visual Studio Code Remote Tunnels for stealth access and improved operational security to evade detection. The attack overlaps with a broader set of cyber incidents documented by Japan's authorities.

Attack Type : Spear-phishing | Cause of Issue : Social Engineering | Industry : Government sector

Top CVE List of March 2025

CVSS Score : 10

Attack Type : Privilege Escalation

01

CVE-2025-2857

A sandbox escape vulnerability in Firefox on Windows allowed a compromised child process to obtain an unintended powerful handle from the parent process, leading to privilege escalation. This vulnerability was actively exploited in the wild. Fixed in Firefox 136.0.4, Firefox ESR 128.8.1, and 115.21.1.

CVSS Score : 8.6

Attack Type : Information Leak

02

CVE-2025-30066

The tj-actions/changed-files GitHub Action versions prior to 46 allowed remote attackers to discover secrets by reading action logs. This was due to a supply chain compromise where tags v1 through v45.0.7 were modified by a threat actor to point at a malicious commit.

CVSS Score : 9.8

Attack Type : Code Execution

03

CVE-2025-24813

Apache Tomcat has a path equivalence issue that could allow a malicious user to view security-sensitive files and/or inject content into those files, potentially leading to remote code execution.

CVSS Score : 10

Attack Type : Code Execution

04

CVE-2025-30364

WeGIA, a web manager for charitable institutions, has a SQL Injection vulnerability that allows the execution of arbitrary SQL commands, compromising stored data.

CVSS Score : 8.5

Attack Type : Privilege Escalation

05

CVE-2025-27440

A heap overflow in some Zoom Workplace Apps may allow an authenticated user to conduct an escalation of privilege via network access.

CVSS Score : 9.8

Attack Type : Bypass

06

CVE-2025-30137

The G-Net GNET APK v2.6.2 has hardcoded credentials for ports 9091, 9092, allowing unauthorized access to the dashcam's API. Once on the GNET SSID, an attacker can send crafted auth commands to get device settings and control it.

CVSS Score : 8.1

Attack Type : Denial of Service

07

CVE-2025-30358

Mesop, a Python UI framework for web apps, before 0.14.1, has a class pollution flaw letting attackers alter global vars and class attributes at runtime. This can cause denial of service (DoS) and role impersonation.

Attack Type : Code Execution

08

CVE-2025-22224

VMware ESXi and Workstation contain a Time-of-Check Time-of-Use (TOCTOU) vulnerability that leads to an out-of-bounds write, potentially allowing local privilege escalation.

Attack Type : Bypass

09

CVE-2025-29927

Next.js, a React framework, has a vulnerability where improper handling of the x-middleware-subrequest header allows attackers to bypass application middleware, potentially leading to unauthorized access.

Attack Type : Code Execution

10

CVE-2025-27607

Python JSON Logger was vulnerable to remote code execution due to a missing dependency, leading to potential code execution when installing development dependencies.

+91 44 4352 4537
contact@briskinfosec.com

+91 7305973769
www.briskinfosec.com