Threatsploit

Adversary Report

March - 2025

Edition - 79

BriskInfosec

VULNERABILITY TO VICTORY

www.briskinfosec.com

Introduction :

Dear Readers,

Welcome to our March Threatsploit Adversary Report. The world of cybersecurity never stands still. Every month, new threats emerge, targeting businesses, individuals, and critical systems in increasingly creative ways. From phishing scams to malware attacks, cybercriminals are finding new ways to exploit vulnerabilities and trick people into handing over sensitive information. Staying informed about these threats is the first step toward protecting yourself and your organization.

This month, we've seen a rise in attacks across various sectors. Banks in India are dealing with a wave of SMS phishing scams designed to steal customer credentials. Gaming platforms like Steam are also under fire, with malicious software disguised as legitimate games stealing passwords. Meanwhile, a sophisticated campaign called REF7707 is exploiting weaknesses in both Windows and Linux systems, posing a serious threat to businesses.

Malware attacks continue to evolve, affecting a range of devices and operating systems. macOS users are facing a new threat called Flexible Ferret malware, which uses clever tricks to bypass security measures. Cloud systems aren't safe either. A new type of attack targeting AWS AMI, known as the whoAMI attack, is putting cloud infrastructure at risk. These incidents highlight how cyber threats are becoming more advanced and harder to detect.

But with the right knowledge and tools, you can stay one step ahead. This report breaks down the latest threats, explains how they work, and provides practical advice to help you strengthen your defenses. By understanding what's out there, you can take action to protect your data, your systems, and your peace of mind.

Best regards,

Briskinfosec Threat Intelligence Team.

Contents :

New Malware Targets Indian Bank Users to Steal Sensitive Financial Data

A sophisticated malware campaign, named "FatBoyPanel," has emerged in India, targeting users of various banks. The malware is distributed via WhatsApp as fake APK files masquerading as legitimate banking or government apps. Once installed, these apps steal sensitive data, including Aadhar numbers, PAN cards, ATM PINs, and credit card details, by mimicking the user interfaces of real banking apps. The malware is designed to intercept and forward SMS messages, including OTPs, to attacker-controlled numbers or Firebase endpoints, enabling unauthorised transactions. The campaign has compromised the data of around 50,000 users, exposing sensitive banking and government details. To protect against this threat, users are urged to only download apps from official app stores, enable multi-factor authentication (MFA), and avoid clicking on suspicious links or downloading unknown attachments. Institutions should also remain vigilant, strengthen security measures, and share information with authorities to track the perpetrators of the campaign.

Attack Type : SMS Phishing

Cause of Issue : Malicious Apps

Industry Type : Banking and Finance

FlexibleFerret Malware Targets macOS Users, Bypasses XProtect Security

A new malware variant, FlexibleFerret, has been discovered targeting macOS users while evading detection by Apple's XProtect. Part of a larger campaign attributed to North Korean threat actors, it spreads through a malicious Apple Installer package named versus.pkg. This package includes harmful components like InstallerAlert.app, versus.app, and a fake zoom binary. The malware communicates with a rogue domain, zoom.callservice[.]us, and installs a persistence item to maintain control. Initially targeting job seekers, the campaign now also affects developers on platforms like GitHub. Users are urged to avoid installing untrusted software and to keep security software updated.

Attack Type : Social Engineering

Cause of Issue : Malicious Installation

Industry Type : Software Sector

PirateFi Game on Steam Distributes Password-Stealing Malware

PirateFi, a free-to-play game on Steam, was found to distribute the Vidar infostealer malware between February 6-12, 2025, affecting up to 1,500 users. The malware, disguised as part of the game, was identified in a file called Pirate.exe and compromised sensitive data like credentials, session cookies, and cryptocurrency wallets. Steam alerted users to run antivirus scans and possibly reinstall Windows. Researchers believe the game's name, referencing web3/blockchain, targeted specific users. Although Steam has security measures like SMS-based verification, the incident highlights vulnerabilities in its protections. Previous cases of malware in Steam games include a 2023 Dota 2 exploit and a compromised mod for Slay the Spire in December 2023.

Attack Type : Infostealer Malware

Cause of Issue : Malicious Game

Industry Type : Media and Entertainment

whoAMI Attack Targets AWS AMI Name Confusion to Achieve Remote Code Execution

Cybersecurity researchers have discovered a new name confusion attack called whoAMI, which targets AWS users. By publishing a malicious Amazon Machine Image (AMI) with a specific name, attackers can exploit misconfigured software to gain remote code execution (RCE) on victim EC2 instances. The attack relies on using the ec2:DescribeImages API without specifying the owner or other filters, allowing attackers to hijack the instance creation process. This technique is a form of supply chain attack, similar to dependency confusion. AWS has addressed the issue, and HashiCorp Terraform now warns users about using the vulnerable search criteria. AWS recommends implementing new security controls, including Allowed AMIs, to mitigate the risk.

Attack Type : Dependency Confusion

Cause of Issue : Misconfigured Filters

Industry Type : Software Sector

REF7707 Campaign Targets Windows and Linux Systems with FINALDRAFT Malware

The REF7707 hacking campaign targets both Windows and Linux systems using novel malware, including FINALDRAFT, GUIDLOADER, and PATHLOADER. The campaign's execution chain begins with certutil downloading files, followed by lateral movement via Windows Remote Management. FINALDRAFT, a key malware component, uses a Windows-signed debugger, CDB.exe, for malicious shellcode injection and persistence. It establishes command and control through Microsoft's Graph API and cloud services, blending in with legitimate traffic. Despite its sophisticated tactics, the attackers' poor operational security exposed pre-production malware and infrastructure. This campaign highlights the need for cross-platform security and vigilance against cloud-based threats.

Attack Type : Advanced Persistent Threat (APT)

Cause of Issue : Security Lapses

Industry Type : Software Sector

New Snake Keylogger Targets Chrome, Edge, and Firefox Browsers

A new variant of the Snake Keylogger (detected as AutoIt/Injector.GTY!tr) is targeting Windows users, utilizing advanced evasion techniques to steal sensitive data from browsers like Chrome, Edge, and Firefox. It employs AutoIt scripting, process hollowing, and multi-channel exfiltration to evade traditional defences. The malware is spread through phishing emails and installs itself in the %Local_AppData%\supergroup directory, with persistence ensured by a VBScript in the %Startup% folder. It injects into RegSvcs.exe to bypass detection and captures keystrokes, banking info, and clipboard data. Exfiltration occurs via SMTP and Telegram. Over 280 million infection attempts have been blocked, with concentrated attacks in several countries. Organisations are urged to use sandboxing, block C2 server connections, and educate users.

Attack Type : Keylogger Injection

Cause of Issue : Phishing Emails

Industry Type : Software Sector

Malicious Go Package Leverages Module Cache for Ongoing Remote Access

Cybersecurity researchers have identified a software supply chain attack targeting the Go ecosystem through a malicious package, github.com/boltdb-go/bolt. This package, a typosquat of the legitimate BoltDB module, was published in November 2021 and cached indefinitely by the Go Module Mirror service. Once installed, the backdoored package allowed remote access to infected systems for arbitrary command execution. Despite the repository being modified later to remove the malicious code, the cached version remained accessible, ensuring continued distribution of the compromised package. The attack highlights the risks of indefinite module caching and mutable Git tags, prompting developers to be vigilant about potential abuse in module repositories.

Attack Type : Typosquatting Attack

Cause of Issue : Mutable Git Tags

Industry Type : Software Sector

Golang Malware Leverages Telegram for Stealthy Command-and-Control Operations

Researchers have discovered a Golang-based backdoor that leverages Telegram for command-and-control (C2) communications. Once executed, the malware checks if it's running as "C:\Windows\Temp\svchost.exe" and if not, it copies itself there and creates a new process to launch it. It utilizes an open-source library for Golang to interact with the Telegram Bot API to receive commands from an actor-controlled chat. The malware currently supports three functional commands: /cmd (executes PowerShell commands), /persist (relaunches itself), and /selfdestruct (deletes itself and terminates). While the /screenshot command exists, it's not fully implemented. The malware's possible Russian origin is suggested by the use of Russian text in the /cmd command. This highlights the challenges defenders face with cloud-based apps, which attackers exploit to complicate detection and response efforts.

Attack Type : Backdoor Trojan

Cause of Issue : Cloud Exploitation

Industry Type : Software Sector

New Mobile Scareware Campaign Promotes Malicious Antivirus Apps

A recent wave of scareware attacks targets mobile users by displaying alarming messages, tricking them into installing malicious antivirus apps. These attacks exploit fear by mimicking legitimate antivirus software and creating a sense of urgency, often claiming devices are infected. Once installed, the malicious app can lead to serious consequences, ranging from harmless programs to malware that steals financial information or encrypts data. The attacks often use fake pop-ups or JavaScript alerts to deceive users. To protect against scareware, users should install genuine antivirus software, keep their devices updated, and avoid downloading apps from unverified sources. Being cautious with suspicious pop-ups can help prevent falling victim to these scams.

Attack Type : Scareware Attack

Cause of Issue : Social Engineering

Industry Type : Telecommunications

North Korean Hackers Exploit Job Interviews to Spread Malware Among Freelance Developers

The DeceptiveDevelopment campaign, attributed to North Korea, targets freelance software developers through job interview lures, primarily via freelancing and job-hunting platforms like Upwork and Freelancer.com. Attackers use fake recruiter profiles to share malicious code hosted on GitHub, GitLab, or Bitbucket, designed to steal cryptocurrency and login information. The malware, including BeaverTail and InvisibleFerret, is delivered through trojanized projects or video conferencing software. InvisibleFerret acts as a backdoor, gathering data from browsers and password managers. The campaign mainly targets developers working on cryptocurrency and decentralized finance projects worldwide, with notable activity in countries like Finland, India, and the U.S. This marks an evolution of North Korea's cybercrime efforts, focusing on cryptocurrency theft.

Attack Type : Spear-phishing Malware | Cause of Issue : Job Scams | Industry Type : Cryptocurrency

Russian Hackers Target Signal Messenger to Access Sensitive Information

The Google Threat Intelligence Group (GTIG) has uncovered a growing campaign by Russia-aligned threat actors targeting Signal Messenger users, primarily Ukrainian military personnel, government officials, journalists, and activists. The attackers exploit Signal's "linked devices" feature to gain persistent access to encrypted communications, bypassing cryptographic protections. Key tactics include manipulating Signal group invitations with malicious JavaScript to link devices without user knowledge. This method leaves no cryptographic traces, requires minimal malware, and avoids traditional command-and-control infrastructure. Signal has released updates to improve phishing detection, but users must enable two-factor authentication and audit linked devices. This tactic, also targeting WhatsApp and Telegram, is expected to spread across secure messaging platforms.

Attack Type : Device Linking | Cause of Issue : Feature Exploitation | Industry Type : Telecommunications

FrigidStealer Malware Targets macOS Through Fake Update Prompts

Cybersecurity researchers have identified a new macOS malware, FrigidStealer, distributed through web injects by the threat actor TA2727. This actor, active since 2022, uses fake update lures to deliver various payloads, including Lumma Stealer on Windows and Marcher banking trojan on Android. FrigidStealer targets macOS users outside North America, prompting them to download a malicious app that bypasses security protections. Written in Go and ad-hoc signed, the malware collects sensitive data from browsers, Apple Notes, and cryptocurrency apps using AppleScript. TA2727 works with TA2726, a traffic distribution system operator, and TA569, which also spreads malware via fake browser updates. This highlights increasing threats targeting both consumer and enterprise systems.

Attack Type : Web Injection | Cause of Issue : Malicious Redirects | Industry Type : Software Sector

Tax-themed Malware Campaign Targets Financial Institutions Globally

A sophisticated malware campaign exploiting the tax season targets financial organizations and individuals globally through phishing emails impersonating tax agencies and financial institutions. The emails, often posing as HMRC, Intuit, or myGov, contain malicious links or attachments that deliver malware and steal credentials. Key malware payloads include Rhadamanthys, which uses PowerShell to install malware, and Voldemort, a backdoor leveraging Google Sheets for communication. This campaign has affected organizations worldwide, including the UK, the US, and Switzerland. To mitigate these threats, organizations should educate employees, implement multi-factor authentication, deploy email filtering, update antivirus software, and monitor for indicators of compromise (IoCs), like phishing and fraud URLs.

Attack Type : Phishing Malware

Cause of Issue : Tax Season

Industry Type : Banking and Finance

Bybit Confirms $1.5 Billion Crypto Theft in Advanced Cold Wallet Attack

On February 21, 2025, Bybit suffered a major hack when over $1.5 billion worth of cryptocurrency, including 400,000 ETH and stETH, was stolen from one of its Ethereum cold wallets. The attack exploited a vulnerability during a routine transfer from a cold to a hot wallet, manipulating the smart contract logic and masking the signing interface. This sophisticated attack, attributed to the Lazarus Group, a North Korean hacker group, marks the largest cryptocurrency heist in history. The attack demonstrates advanced techniques, including social engineering and interface manipulation, targeting institutional multisig setups. While other cold wallets remain secure, Bybit has reported the incident to authorities and is working with cybersecurity firms to investigate the breach.

Attack Type : Interface Manipulation

Cause of Issue : Smart Contract Manipulation

Industry Type : Cryptocurrency

Chinese Cyber Group Leverages MAVInject.exe to Evade Antivirus Detection

Mustang Panda, a Chinese state-sponsored cyber group, is using new techniques to evade detection. The group employs Microsoft's MAVInject.exe to inject malicious code into processes, bypassing ESET antivirus by using "waitfor.exe." The attack sequence starts with a dropper executable ("IRSetup.exe") that installs malware and a decoy PDF, often targeting users in Thailand through spear-phishing. The malware, a variant of TONESHELL, sideloads a rogue DLL via a legitimate EA application. It connects to a remote server for commands, enabling file movement and deletion. ESET responded, stating their software has long protected against this attack. Separately, Bookworm malware, linked to Mustang Panda, has been seen targeting ASEAN countries with DLL side-loading techniques.

Attack Type : Fileless Malware

Cause of Issue : Malicious Injection

Industry Type : Government Sector

Xerox Printer Vulnerabilities Could Expose Windows Active Directory Credentials to Attackers

Security vulnerabilities have been found in Xerox VersaLink C7025 Multifunction printers, affecting firmware versions 57.69.91 and earlier. These vulnerabilities allow attackers to capture authentication credentials through pass-back attacks via LDAP and SMB/FTP services. CVE-2024-12510 (CVSS 6.7) allows credential redirection via LDAP, while CVE-2024-12511 (CVSS 7.6) allows attackers to capture SMB/FTP credentials by modifying the address book configuration. Successful exploitation requires physical or remote access to the printer console. Xerox addressed these issues in Service Pack 57.75.53. Also, a flaw called unauthenticated SQL injection (CVE-2024-56735) was found in HealthStream MSOW. This means that sensitive data from 23 healthcare organisations could be accessed by anyone on the internet.

Attack Type : Pass-back Attack

Cause of Issue : Configuration Vulnerability

Industry Type : Healthcare

Microsoft Discovers Advanced XCSSET Malware Variant Targeting macOS with Improved Obfuscation

Microsoft has discovered a new variant of the XCSSET macOS malware, marking its first major update since 2022. This version introduces enhanced obfuscation, updated persistence mechanisms, and new infection strategies. XCSSET targets digital wallets and exfiltrates data from apps like Google Chrome, Telegram, Notes, and more. Initially discovered in 2020, XCSSET spreads via infected Xcode projects and has adapted to newer macOS versions, including M1 chipsets. The latest variant adds advanced persistence by replacing the legitimate Launchpad with a malicious version, ensuring the malware runs with every session. Users are advised to verify downloaded Xcode projects and only install apps from trusted sources to protect against the malware.

Attack Type : Malware Infection

Cause of Issue : Xcode Vulnerabilities

Industry Type : Software Sector

Hackers Exploit CAPTCHA in Webflow CDN PDFs to Evade Detection

A phishing campaign has been exploiting Webflow's CDN to steal credit card information. Attackers trick victims searching for documents on search engines, leading them to malicious PDFs. These PDFs contain an embedded CAPTCHA image that redirects users to a phishing page with a real Cloudflare Turnstile CAPTCHA, creating a false sense of legitimacy. After completing the CAPTCHA, victims are prompted to enter credit card details on a fake download page, but when the details are submitted, an error is shown. Multiple attempts redirect users to a 500 error page. Meanwhile, a new phishing kit named Astaroth, sold for $2,000, allows cybercriminals to harvest login credentials and bypass two-factor authentication (2FA) using a reverse proxy to intercept traffic between victims and legitimate services like Gmail and Microsoft.

Attack Type : Phishing Attack

Cause of Issue : Malicious PDFs

Industry Type : Banking and Finance

North Korean Cybercriminals Use PowerShell Exploit to Take Control of Devices

A North Korea-linked hacker group, Kimsuky, is using a new tactic to deceive victims into running malicious PowerShell commands. Posing as South Korean officials, they send spear-phishing emails with a PDF attachment, leading victims to a registration link that instructs them to run malicious code. This downloads a remote desktop tool and certificate, enabling the attackers to exfiltrate data. The technique, observed since January 2025, marks a shift from Kimsuky's usual methods. Additionally, a U.S. woman, Christina Marie Chapman, pleaded guilty for helping North Korean IT workers fraudulently obtain remote jobs at over 300 U.S. companies, generating over $17.1 million. The scheme also led to data exfiltration and extortion.

Attack Type : Social Engineering

Cause of Issue : Phishing Attack

Industry Type : Software Sector

Grubhub Reports Breach Exposing Customer and Driver Data

Grubhub, a major U.S. food delivery platform, reported a data breach after hackers accessed personal details of customers, merchants, and drivers via a third-party service provider. The breach affected users, including those of Grubhub's Campus Dining service. Personal information compromised includes names, emails, phone numbers, partial payment card details (last four digits), and hashed passwords for legacy systems. However, bank account details and Social Security numbers were not exposed. Grubhub detected "unusual activity" and promptly terminated the compromised provider's access. The company did not disclose how many individuals were impacted or when the breach occurred. Grubhub, recently acquired by Wonder Group for $650 million, operates across 4,000 U.S. cities.

Attack Type : Third-party Breach

Cause of Issue : Unauthorized Access

Industry Type : Food and Beverages

Hackers Use Google Tag Manager to Inject Credit Card Skimmers on Magento Websites

Threat actors are exploiting Google Tag Manager (GTM) to deliver credit card skimmer malware targeting Magento-based e-commerce sites. The malware, hidden in an obfuscated GTM script, allows persistent attacker access and steals credit card details during checkout, sending them to an external server. Sucuri reported a decrease in infected sites, with three still affected by the malicious GTM identifier (GTM-MLHK2N68). The malware is loaded from the Magento database's "cms_block.content" table. This isn't the first GTM abuse-previously, it was used in a malvertising campaign. In a related case, two Romanian nationals face charges for their involvement in a payment card skimming operation. If convicted, they face significant prison time and fines.

Attack Type : Credit card Skimming

Cause of Issue : Malicious Script

Industry Type : E-Commerce

Malicious ML Models on Hugging Face Exploit Corrupted Pickle Files to Avoid Detection

Cybersecurity researchers discovered two malicious machine learning models on Hugging Face, using a technique called "nullifAI" to bypass detection. The models, stored in PyTorch format, contained "broken" pickle files, which execute malicious payloads (a reverse shell) when deserialized. Pickle files are often used for serializing ML models but can run arbitrary code during deserialization, posing a security risk. These malicious models were compressed using the 7z format instead of the default ZIP format, allowing them to evade detection by Picklescan, a tool designed to identify suspicious pickle files. The attack leverages the fact that the malicious payload is inserted early in the pickle file's stream, enabling it to execute before the file is flagged as unsafe. This makes the models harder to detect. The discovered models are considered proof-of-concept rather than part of a large-scale attack. Hugging Face has since updated its security tools to address this vulnerability.

Attack Type : Reverse Shell

Cause of Issue : Serialization Flaw

Industry Type : AI and Machine Learning

Microsoft Uncovers 3,000 Exposed ASP.NET Keys Fueling Code Injection Vulnerabilities

Microsoft has warned of a security risk where software developers use publicly disclosed ASP.NET machine keys from accessible resources, potentially exposing applications to attacks. Threat actors exploited these keys in December 2024 to deliver the Godzilla post-exploitation framework through ViewState code injection attacks. Over 3,000 publicly disclosed keys have been identified, posing a higher risk than previously known attacks using compromised keys. If these keys are exposed, attackers can exploit them to execute malicious code on the target server. Microsoft advises against using publicly available keys, recommends regular key rotation, and emphasizes that rotating keys alone may not fully mitigate the risk if persistence is established. Additionally, Aqua's research revealed a Kubernetes vulnerability that can bypass security policies, enabling unauthorized container image deployments.

Attack Type : ViewState Injection

Cause of Issue : Publicly Disclosed Keys

Industry Type : Software Sector

Fake Chrome Websites Deliver ValleyRAT Malware Using DLL Hijacking

Bogus websites advertising Google Chrome have been used to distribute the ValleyRAT remote access trojan (RAT), first detected in 2023. The malware, attributed to the Silver Fox threat actor, primarily targets Chinese-speaking regions and key roles in organizations, such as finance and sales. Attackers use counterfeit Chrome installers to deploy ValleyRAT, often alongside other malware like Gh0st RAT and Purple Fox. These fake sites exploit users' trust in legitimate software downloads, leading to infections. Upon execution, ValleyRAT collects sensitive data, logs keystrokes, and establishes persistence. It communicates with remote servers to download additional payloads and execute arbitrary code. The campaign also uses drive-by download schemes and malicious installer packages to deploy the malware, often through DLL hijacking techniques.

Attack Type : Malicious Download

Cause of Issue : Fake Installers

Industry Type : Banking and Finance

SparkCat Malware Exploits OCR to Steal Crypto Wallet Phrases from Images

A new malware campaign, SparkCat, has been discovered, targeting both Apple's App Store and Google Play to steal cryptocurrency wallet recovery phrases. The malware uses an optical character recognition (OCR) model to extract images containing wallet mnemonics from photo libraries and sends them to a command-and-control server. SparkCat masquerades as AI, food delivery, and Web3 apps, with over 242,000 downloads on Google Play. The campaign primarily targets Europe and Asia, with a threat actor believed to be fluent in Chinese. In addition, another malware campaign called FatBoyPanel, affecting Android users in India, harvests sensitive financial information via malicious APKs. The apps have since been removed from both stores, and Google Play Protect provides protection against known versions.

Attack Type : OCR-based Exfiltration

Cause of Issue : Malicious Apps

Industry Type : Cryptocurrency

Russian Hackers Exploit 7-Zip Vulnerability to Bypass Windows MotW Protections

A recently patched security vulnerability in 7-Zip (CVE-2025-0411) was exploited by cybercriminals to deliver SmokeLoader malware. The flaw bypasses Microsoft's MotW protections by allowing remote attackers to execute malicious code through double-archived files. Exploited in spear-phishing campaigns, the flaw targeted the Ukrainian government and business organizations, using homoglyph attacks to disguise malicious files. The attack chain starts with phishing emails containing a ZIP file that tricks users into executing a malicious.URL file, leading to SmokeLoader. At least nine Ukrainian entities were impacted. The financially motivated UAC-0006 group also targeted PrivatBank in a similar campaign. Users are advised to update 7-Zip, implement email filtering, and disable execution of untrusted files to mitigate risk.

Attack Type : Spear-phishing Attack

Cause of Issue : MotW Bypass

Industry Type : Government Sectors

Coyote Malware Grows: Targets Over 1,000 Sites and 70 Financial Entities

A new banking malware called Coyote is targeting Brazilian Windows users, capable of keylogging, capturing screenshots, and displaying phishing overlays to steal credentials. Discovered by Fortinet, the malware is delivered via Windows Shortcut (LNK) files that execute PowerShell commands to retrieve malicious payloads from a remote server. Coyote can steal sensitive information from over 1,000 websites, including 70 financial agents like mercadobitcoin.com.br and bitcointrade.com.br. The malware creates persistence by modifying the Windows registry and exfiltrates system and antivirus data to remote servers. It checks for sandboxes and virtual environments to avoid detection and activates keyloggers and overlays when victims access targeted sites. Coyote's complex, multi-stage infection process poses a significant threat to financial cybersecurity in Brazil.

Attack Type : Banking Trojan

Cause of Issue : Malicious Payload

Industry Type : Banking and Finance

Chinese Cyber Espionage Group Targets Industrial Sectors with FatalRAT Malware

A cyberespionage campaign using the FatalRAT remote access trojan (RAT) is targeting industrial organizations in the Asia-Pacific region, including Taiwan, China, Japan, Thailand, and Singapore. The attackers, believed to be Chinese-speaking, use legitimate Chinese cloud services (e.g., Youdao Cloud Notes and Tencent Cloud) to distribute malware and evade detection. The infection begins with phishing emails disguised as tax documents, containing ZIP archives that deploy a multi-stage infection process. The RAT logs keystrokes, exfiltrates data, and enables remote execution of commands. Kaspersky recommends network segmentation and monitoring DLL sideloading to defend against this threat.

Attack Type : Remote Access

Cause of Issue : Phishing Emails

Industry Type : Energy and Utilities

Cisco Reveals Salt Typhoon Used CVE-2018-0171 to Compromise U.S. Telecom Networks

Cisco confirmed that the Chinese threat actor, Salt Typhoon, exploited the CVE-2018-0171 vulnerability and stolen credentials to target U.S. telecommunications companies. The group maintained persistent access for over three years, using sophisticated techniques like capturing SNMP, TACACS, and RADIUS traffic to obtain more credentials. They employed living-off-the-land tactics to pivot between telecoms and altered network configurations for remote access via SSH. A custom tool, JumbledPath, was used to execute packet captures and clear logs to obfuscate traces. Salt Typhoon also manipulated the loopback interface on switches to bypass access control lists (ACLs). Cisco found no evidence of other known vulnerabilities being exploited, but identified additional attacks on devices with exposed Smart Install (SMI) using CVE-2018-0171.

Attack Type : Advanced Persistent Threat (APT)

Cause of Issue : Stolen Credentials

Industry Type : Telecommunication Sector

China-Linked Hackers Target Check Point Vulnerability to Deploy ShadowPad and Ransomware

A cyber espionage campaign, codenamed Green Nailao, targeted European organizations, especially in the healthcare sector, using the Check Point network gateway vulnerability (CVE-2024-24919). The attackers deployed ShadowPad and PlugX malware, leading to the installation of NailaoLocker ransomware. The threat actors used DLL side-loading techniques and remote desktop protocol (RDP) for lateral movement. The ransomware encrypted files and demanded a bitcoin ransom. The campaign is linked to Chinese-aligned threat actors due to the use of ShadowPad and tradecraft similar to that of the Bronze Starlight group. Trend Micro also observed the malware evolving with anti-debugging and encryption improvements. The campaign targeted 21 companies across 15 countries and multiple sectors. The threat's ultimate aim remains unclear, but it's speculated to be a mix of espionage and opportunistic ransom.

Attack Type : Ransomware Attack

Cause of Issue : Vulnerable Gateway

Industry Type : Healthcare Domain

Top CVE List of February 2025

1.CVE-2025-27364

This vulnerability occurs due to insecure handling of agent compilation requests in Caldera's server API. Attackers can send a specially crafted web request using the gcc -extldflags linker flag to execute arbitrary commands. The flaw allows remote code execution (RCE) because user-controlled inputs are processed without proper validation in the implant compilation function.

AFFECTED PRODUCT: MITRE Caldera ≥ 5.0.0

VULNERABILITY TYPE: Remote Code Execution

2. CVE-2025-26793

The default credentials (freedom / viscount) in the Web GUI of Enterphone MESH remain unchanged after installation, and the system does not enforce a password reset. Attackers can exploit this weakness to log in remotely and access sensitive resident data from multiple buildings. The issue persists due to poor security configuration and user negligence in updating credentials.

AFFECTED PRODUCT: Hirsch Enterphone MESH

VULNERABILITY TYPE: Default Credentials

3. CVE-2025-26617

A SQL Injection flaw exists in the historico_paciente.php endpoint of WeGIA. The application fails to properly sanitize user inputs, allowing attackers to inject and execute arbitrary SQL queries. This could result in unauthorized access to patient records, data leakage, or manipulation of stored information. The vulnerability occurs due to missing input validation on database queries.

AFFECTED PRODUCT: WeGIA Web Manager

VULNERABILITY TYPE: SQL Injection

4. CVE-2025-25675

Score : 9.8

The router's formexeCommand function directly processes user-supplied input without proper sanitization. The cmdinput parameter is passed to doSystemCmd, allowing attackers to inject and execute arbitrary system commands. This happens due to improper handling of input variables, leading to a critical command injection flaw.

AFFECTED PRODUCT

Tenda AC10 Router

VULNERABILITY TYPE

Command Injection

5. CVE-2025-25746

Score : 9.8

A stack-based buffer overflow vulnerability exists in the SetWanSettings module of D-Link DIR-853. Attackers can supply an oversized input for the Password parameter, leading to memory corruption and potential remote code execution. This issue occurs due to lack of bounds checking, allowing exploitation through a carefully crafted request.

AFFECTED PRODUCT

D-Link DIR-853 Router

VULNERABILITY TYPE

Buffer Overflow

Know the threats before they know you

+91 44 4352 4537 | +91 73059 79769
contact@briskinfosec.com | www.briskinfosec.com