Briskinfosec's

# Threatsploit Adversary Report

December 2025

88th Edition

BriskInfosec™

VULNERABILITY TO VICTORY

# Introduction :

## Dear Readers,

Every month, breaches and weapon-ready vulnerabilities quietly reshape digital risk. Warning signs are rare, detection is late, and a single miss can disrupt a business in minutes. Cyber risk is no longer only technical, it’s a matter of survival.

Welcome to our December edition, your tactical window into global cybersecurity landscape. This edition brings a clean and focused intelligence brief, covering ransomware strikes, mass identity exposure, perimeter compromises, and critical software flaws being weaponized faster than patch cycles can follow.

Many real incidents stood out last month, not because they were isolated, but because they showed us how the attacker mindset is changing. The PowerSchool SIS Data Breach alone exposed millions of student and staff records, impacting trust across the education sector. The Prudential Financial cyberattack confirmed that identity-heavy repositories are still a favorite target, reaching employee and contractor data.

At the same time, attacks tied to specific sectors and network edges increased. The Rhysida healthcare ransomware campaign showed the growing pressure on medical networks, the Cisco ASA VPN exploit proved that attackers now lean toward trusted access points, and the ActiveMQ RCE attack revealed how middleware messaging platforms have turned into execution surfaces for remote takeover.

If there’s a single lesson to take forward, it’s this : Security isn’t shaped by the number of alerts you receive, but by the threats you understand at the right time. Awareness gives direction, timing gives advantage, and context becomes the difference between reacting and responding with control.

Best regards,

Briskinfosec Threat Intelligence Team.

### Highlights

## Checking the actual security of Google Workspace

This article examines the actual security of Google Workspace by highlighting common risks, misconfigurations, and overlooked settings that can expose organizations to threats. It explains how attackers take advantage of weak controls and what IT teams should verify to keep accounts, data, and access safe. Practical steps are included to help strengthen defences and maintain a secure workspace environment.

Attack Type : Misconfiguration Exploitation

Cause of Issue : Vulnerable Configuration

Industry : IT/Enterprise

## Chrome Zero Day Used to Install Spyware Through Compromised Websites

Attackers exploited a zero-day vulnerability in Google Chrome that bypassed the browser sandbox and delivered spyware when users visited malicious websites. The campaign targeted high-value sectors and relied on a crafted webpage to trigger the exploit, granting attackers deeper system access. Google patched the flaw, but active exploitation highlights the ongoing risks from browser-based zero-day attacks.

Attack Type : Zero-day Exploitation

Cause of Issue : Chrome Sandbox Bypass

Industry : Media, Government Agency

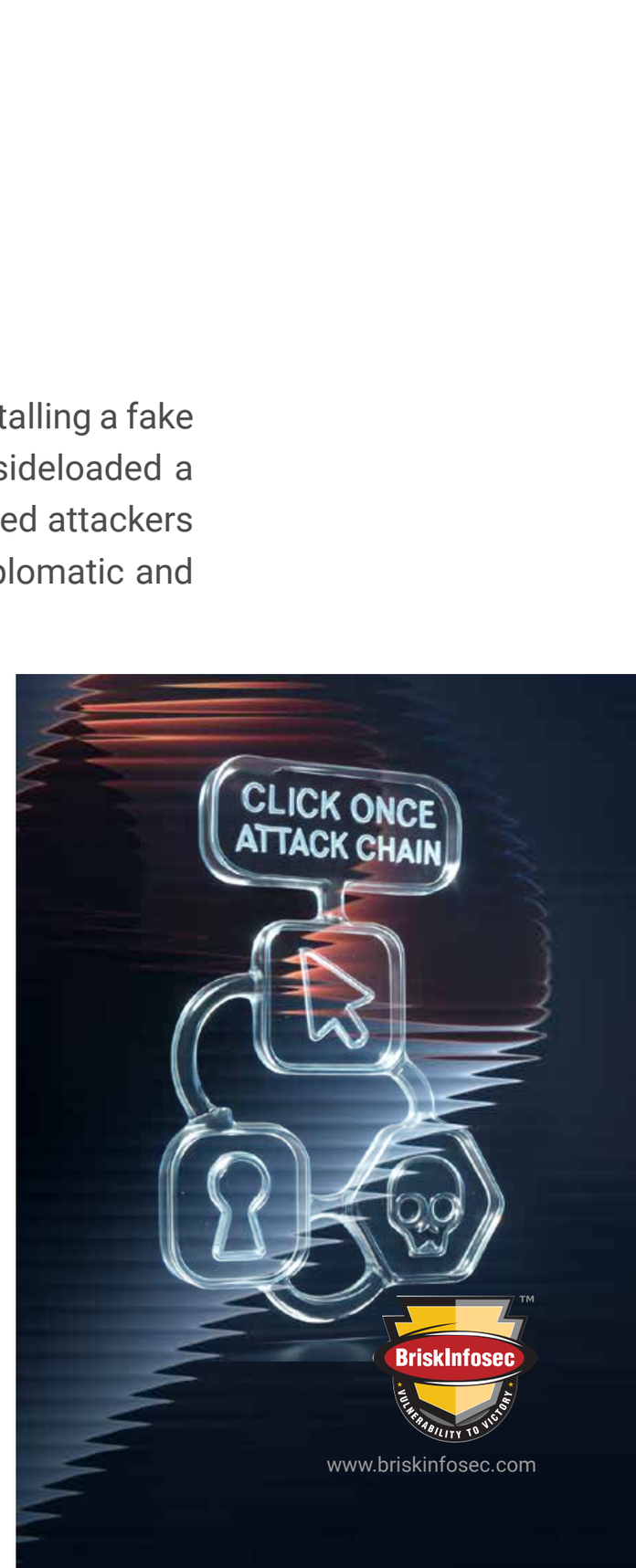
## SideWinder Uses New ClickOnce Attack Chain to Target South Asian Diplomats

A spear-phishing campaign by SideWinder delivered malicious PDFs that tricked recipients into installing a fake “Adobe Reader update.” Instead of Reader, victims downloaded a ClickOnce application, which sideloaded a malicious DLL and launched malware (ModuleInstaller → StealerBot). The spyware implants allowed attackers to exfiltrate sensitive files, capture keystrokes, and run remote shells. The campaign targeted diplomatic and governmental organisations across South Asia.

Attack Type : Spear-Phishing

Cause of Issue : Deceptive PDF

Industry : Government, Embassy



## ChatGPT Atlas Browser Exploit Lets Attackers Embed Persistent Hidden Commands

Researchers discovered a vulnerability in ChatGPT Atlas that allows attackers to inject persistent, hidden instructions into the AI assistant's memory via a malicious web page. Once the user interacts with ChatGPT later, those tainted instructions trigger arbitrary code execution or other malicious actions - often without leaving obvious traces. The flaw exposes serious security risks for users of AI-powered browsers.

Attack Type : Memory Injection

Cause of Issue : Session Memory Injection

Industry : IT/Enterprise

## Qilin Ransomware Now Uses Linux Payload on Windows via BYOVD Attack

Qilin ransomware now delivers a Linux-based payload that runs on Windows systems via remote-management tools and driver exploits. Attackers first gain access, often using stolen credentials then sideload a vulnerable driver, bypass security controls, and deploy ransomware along with data exfiltration tools. The attack chain ends with file encryption and deletion of backups, leaving victims unable to recover without paying ransom. This hybrid method makes Qilin especially dangerous for organisations using mixed OS environments or remote-management infrastructure.

Attack Type : Ransomware

Cause of Issue : Credential Compromise

Industry : Manufacturing

## Botnet Attacks Surge : PHP Servers & IoT Devices Under Heavy Scan

Security researchers warn that automated botnet attacks are sharply increasing, targeting exposed PHP servers, IoT devices and cloud gateways. Threat actors using botnets such as Mirai, Gafgyt and Mozi  are launching high-volume scans and exploitation attempts to compromise poorly secured web servers and devices. The rise underlines the need for organizations to harden default credentials, apply patches promptly, and limit exposure of internet-facing services.

Attack Type : Automated Scanning

Cause of Issue :  Public-facing PHP & IoT Services

Industry : Infrastructure

## Russian Hackers Use Webshells and Living-Off-The-Land Tactics Against Ukrainian Networks

Threat actors of Russian origin targeted a business-services firm and a local government entity in Ukraine, deploying webshells on public-facing servers to gain access. Once inside, they used legitimate OS tools and dual-use software  rather than heavy malware to move laterally, dump memory, evade malware scans, and exfiltrate sensitive data. The low-footprint, stealth-first approach helped them remain undetected for weeks.

Attack Type : Living-Off-The-Land

Cause of Issue : Unpatched Server Vulnerability

Industry : Government


## Malicious npm Packages Found Stealing Developer Credentials

Security researchers discovered ten typosquatted npm packages that delivered a multi-stage information stealer targeting Windows, macOS, and Linux. The packages displayed a fake CAPTCHA to appear legitimate, then downloaded an obfuscated payload that harvested credentials from system keyrings, browsers, and authentication services. The campaign accumulated nearly 10,000 downloads before detection, highlighting serious risks in software supply chain security.

Attack Type : Supply-chain Malware

Cause of Issue : Typosquatted Packages

Industry : Development

## Active Exploits Target DELMIA Apriso and XWiki Platforms

Security agencies confirm that multiple critical vulnerabilities in DELMIA Apriso and XWiki are under active exploitation including code-injection, missing-authorization and eval-injection flaws. Attackers use these flaws to execute arbitrary code, escalate privileges or drop malicious payloads (such as coin miners) on compromised servers. The exploitation chain threatens remote-access systems, enterprise collaboration tools, and data integrity for affected organisations worldwide.

Attack Type : Remote-Code Execution

Cause of Issue :  Input Injection

Industry : Enterprise


BriskInfosec
VULNERABILITY TO VICTORY

www.briskinfosec.com

## Herodotus Android Trojan Outsmarts Fraud Detection by “Typing Like a Human”

Herodotus is a new Android banking trojan that uses a dropper app distributed via SMS-phishing to trick users into installing it. Once installed, it abuses accessibility services and overlays fake banking login screens to steal credentials and 2FA codes. What makes it dangerous is its human-like behaviour : the malware simulates real typing (with random delays and screen interactions) to bypass behaviour-based fraud detection systems.

Attack Type : Banking Trojan

Cause of Issue : Social Engineering

Industry : Mobile Software

## GhostCall & GhostHire : Fake Zoom-Calls and Job Lures Target Web3 Firms

Research shows that GhostCall and GhostHire run by a subgroup of BlueNoroff use fake video-call invites or bogus recruitment lures to trick victims into installing malware. GhostCall sends phishing invites to alleged Zoom/Teams meetings; GhostHire offers fake job assignments to Web3 developers. Once installed, malicious loaders drop credential-stealers, backdoors and spyware on macOS or Windows devices. Targets span crypto firms, blockchain tech teams, and executives globally.

Attack Type : Malware Delivery

Cause of Issue : Job-offer fraud

Industry : Crypto

## Top Black Friday Cybersecurity and IT Deals for 2025

This article highlights major Black Friday 2025 discounts on cybersecurity tools including VPNs, antivirus suites, password managers, data protection software and IT utilities. It lists top offers from leading vendors and explains how individuals and organisations can benefit from upgrading security solutions at reduced prices. The deals cover privacy tools, device protection, online safety products and enterprise-friendly software options.

Attack Type : Social Engineering

Cause of Issue :  Seasonal Security Promotions

Industry : Consumer Technology

## GlassWorm Malware Resurfaces in VS Code Extensions on OpenVSX

GlassWorm has returned on the OpenVSX registry with three new malicious VS Code extensions, already downloaded over 10,000 times. The malware uses invisible Unicode characters to hide malicious JavaScript code, steals credentials (GitHub, npm, OpenVSX) and crypto-wallet data, and installs proxy or remote-access tools on infected developer machines. The campaign spreads through supply-chain infection of extensions affecting developers globally, and potentially turning compromised systems into criminal infrastructure.

Attack Type : Malware

Cause of Issue : Malicious Extensions

Industry : Development

## QNAP Patches Seven Critical NAS Zero-Days After Pwn2Own 2025

QNAP fixed seven critical zero-day vulnerabilities discovered and exploited at the Pwn2Own Ireland 2025 competition. The flaws impacted its QTS and QuTS-hero operating systems, and key apps like Hyper Data Protector, Malware Remover and Hybrid Backup Sync. If left unpatched, the vulnerabilities could allow remote code execution, unauthorized access to backups or complete device compromise. Users are urged to update immediately to the patched versions to avoid potential data theft or NAS takeover.

Attack Type : Remote-Code Execution

Cause of Issue : Memory Corruption

Industry : Networking

## Leak Suggests Google Gemini 3 Pro and Nano Banana 2 Launch Is Imminent

Recent leaks show that Nano Banana 2 (codename “GEMPIX2”) and Gemini 3 Pro could launch as soon as December 2025. Nano Banana 2 is expected to deliver enhanced image-generation and editing capabilities, including higher resolution, better text rendering, and improved world knowledge. The leak has sparked anticipation among developers, designers and AI tool users awaiting next-gen image and AI models from Google.

Attack Type : Data Leak

Cause of Issue : Premature Disclosure

Industry : AI

## APT37 Abuses Google Find Hub to Wipe Android Devices Remotely

North Korea-linked threat actors used phishing via a messaging app to infect victims' PCs. After stealing Google account credentials, they hijacked Google Find Hub to track targets' GPS location and remotely wipe their Android devices, deleting data and disabling alerts. The campaign targeted South Korea, and used the wipe to cover traces and further propagate malware via the victim's messenger contacts.

Attack Type : Credential Theft

Cause of Issue : Credential Compromise

Industry : Telecom

## CISA Orders Patching of Samsung Zero-Day Used in Spyware Attacks

CISA has directed U.S. federal agencies to patch a critical zero-day vulnerability in Samsung's image-processing library, tracked as CVE-2025-21042. The flaw was actively exploited in the wild to deliver the spyware LandFall via malicious DNG image files sent over messaging apps. If unpatched, attackers could achieve remote code execution on affected Samsung devices, enabling data theft, call and location tracking, and deep device compromise. The advisory urges immediate updates to mitigate ongoing risks.

Attack Type : Zero-day Exploitation

Cause of Issue : Image-Processing Flaw in Samsung

Industry : Mobile Software

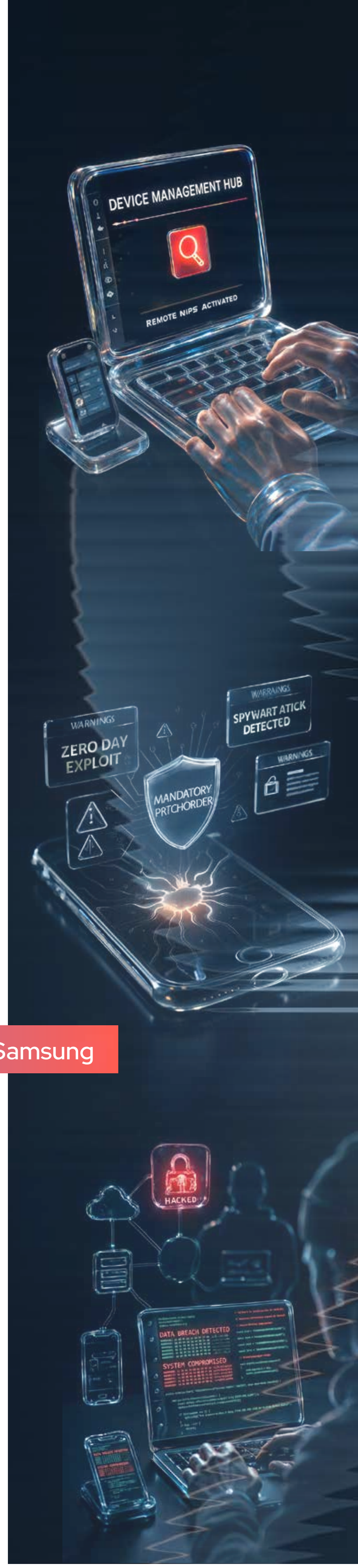
## Yanluowang Initial-Access Broker Pleads Guilty to Ransomware Attacks

A Russian national admitted guilt for acting as the initial-access broker (IAB) for Yanluowang ransomware attacks against multiple US firms between July 2021 and November 2022. The broker sold stolen credentials and network access, which ransomware operators used to infiltrate corporate networks, encrypt data and demand ransoms. Investigators recovered chat logs, cryptocurrency payment trails, and login credentials linking the suspect to several high-value attacks. He faces decades in prison and over $9 million in restitution.

Attack Type : Ransomware

Cause of Issue : Credential Theft

Industry : Corporate



## Why LinkedIn Has Become a Prime Phishing Target

Phishing attacks are increasingly shifting from email to social networking platforms like LinkedIn. Attackers exploit LinkedIn direct messages to bypass traditional email filters, using social-engineering tactics to reach executives and employees on corporate devices. Because LinkedIn is often accessed from work laptops or phones, malicious links or fake recruiter messages can give attackers a foothold into corporate accounts. The trend underlines how phishing has moved beyond email and shows the need for broader security controls across social and business apps.

Attack Type : Phishing

Cause of Issue : LinkedIn-based Phishing Outreach

Industry : Technology


## runC Flaws Could Let Hackers Escape Docker Containers

Three new high-severity flaws in runC-the core container runtime used by frameworks like Docker and Kubernetes - have been disclosed. These vulnerabilities (CVE-2025-31133, CVE-2025-52565, CVE-2025-52881) can allow a malicious container to break out of isolation and gain root-level access to the host system. Attackers exploiting these could write to critical host files, escalate privileges, or take over entire systems. Organisations using containerised environments are urged to update runC immediately to patched versions.

Attack Type : Privilege Escalation

Cause of Issue : Runtime Isolation Flaw

Industry : Cloud Sector

## Russian Ransomware Gangs Weaponize Open-Source AdaptixC2 Framework

Security researchers report that several Russian-linked ransomware groups are now using the open-source post-exploitation tool AdaptixC2 as a command-and-control framework. Originally built for penetration testing and red-teaming, this tool is being abused in live ransomware campaigns. Enabling attackers to manage compromised assets, deploy payloads and orchestrate attacks stealthily. The shift underlines how legitimate open-source tools are being repurposed as powerful weapons in criminal toolchains.

Attack Type : Post-Exploitation

Cause of Issue : Legitimate Open-Source Tool Abuse

Industry : Cloud Sector


BriskInfosec
VULNERABILITY TO VICTORY
www.briskinfosec.com

## U.S. Prosecutors Indict Cybersecurity Insiders Over BlackCat Ransomware Attacks

U.S. federal prosecutors have charged three cybersecurity professionals with conspiring to run ransomware attacks using BlackCat (aka ALPHV) against at least five companies between May and November 2023. The accused worked in incident-response and ransomware negotiation firms but are alleged to have used their access and expertise to breach victim networks, deploy ransomware, steal data, and extort payment in cryptocurrency. The case underscores how trusted insiders and security professionals can be turned into threat actors.

Attack Type : Ransomware

Cause of Issue : Insider threat

Industry : Corporate Sector

## Microsoft Detects SesameOp Backdoor Using OpenAI API as Covert C2

Researchers at Microsoft uncovered “SesameOp,” a backdoor malware that abuses the OpenAI Assistants API as a stealth command-and-control channel. Instead of using traditional infrastructure, the malware fetches encrypted commands via the API and executes them locally. The implant uses obfuscated .NET libraries and internal web shells to maintain persistence. The discovery shows attackers are now repurposing legitimate AI-service APIs to perform espionage and long-term control over compromised systems.

Attack Type : Stealth Backdoor

Cause of Issue : API abuse

Industry : Enterprise

## Cybercriminals Exploit Remote Monitoring Tools to Raid Logistics Networks

Cybercriminals are abusing legitimate Remote Monitoring and Management (RMM) tools to infiltrate trucking and logistics firms. They distribute malicious installers disguised as freight job leads, then deploy tools like ScreenConnect and PDQ Connect to gain remote access. Once inside, attackers harvest credentials, manipulate dispatch systems, and hijack real cargo shipments. The operations combine cyber compromise with physical theft, targeting supply-chain and freight networks for financial gain.

Attack Type : Supply-Chain

Cause of Issue : Malicious RMM installation

Industry : Logistics

## Nation-State Hackers Launch “Airstalk” Malware in Supply Chain Attack

Security researchers say a nation-state–linked group is deploying a new malware named Airstalk via a suspected supply-chain attack. Airstalk abuses the API of a mobile device management platform (AirWatch / Workspace ONE UEM) to create a covert command-and-control channel. Once installed, it can exfiltrate browser cookies, history, bookmarks, screenshots, and other user data bypassing traditional detection systems by using legitimate MDM APIs and stolen certificates. The malware exists in PowerShell and .NET variants, increasing its threat to enterprise environments.

Attack Type : Supply-Chain

Cause of Issue : MDM API Abuse

Industry : Enterprise Sector

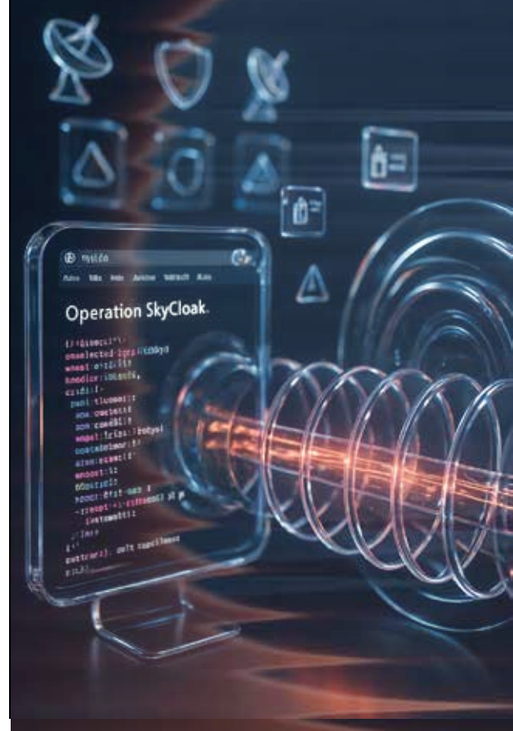

## Operation SkyCloak Uses Tor-Enabled OpenSSH Backdoor to Target Defence Networks

Threat actors behind Operation SkyCloak are deploying a backdoor that uses a hardened OpenSSH service combined with a Tor hidden-service (with obfs4) to hide command-and-control traffic. The attack begins with phishing emails luring targets into opening a ZIP containing a malicious LNK launching a multi-stage infection that installs sshd.exe and a customized Tor binary. Once deployed, attackers gain persistent, stealthy remote access, SMB/SSH tunnel access, and data exfiltration capabilities. The campaign appears aimed at defence-sector organisations in Russia, Belarus and other sensitive targets

Attack Type : Backdoor

Cause of Issue : Legitimate Open-Source Tool Abuse

Industry : Defense Sector




## Trojanized ESET Installers Deliver Kalambur Backdoor in Phishing Attacks

Attackers impersonated the security vendor’s brand and sent phishing emails or Signal messages with links to trojanized installers of a known antivirus tool. The installer drops the legitimate antivirus remover plus a hidden backdoor called Kalambur (also known as SUMBUR), which uses the Tor network for covert command-and-control. The malware also enables remote-access tools (SSH, RDP), allowing persistent access on compromised systems. Victims were primarily in Ukraine.

Attack Type : Supply-Chain

Cause of Issue : Malicious Installer Impersonation

Industry : Security Domain


BriskInfosec
VULNERABILITY TO VICTORY
www.briskinfosec.com

## Cisco Warns of New Firewall Attack Exploiting Critical ASA/FTD Vulnerabilities

Cisco issued a security alert after attackers exploited two zero-day flaws in its Secure Firewall ASA and FTD products (CVE-2025-20333, CVE-2025-20362). The vulnerabilities allow remote attackers to execute arbitrary code or bypass authentication via HTTP(S) requests. Recent attacks caused unexpected device reloads (Denial-of-Service) and enabled deployment of malware such as RayInitiator and LINE VIPER. Organisations using affected firewalls are urged to patch immediately to prevent potential full-device takeover.

Attack Type : Remote-Code Execution

Cause of Issue : Input-Validation Flaw

Industry : Networking Sector

## Fantasy Hub Android RAT Turns Telegram into Malware-as-a-Service Hub

Researchers uncovered Fantasy Hub, a new Android remote-access trojan sold on Russian-language Telegram under a Malware-as-a-Service model. The malware delivers spyware hidden in trojanized apps or fake “Google Play update” packages. Once installed and granted default SMS-handler privileges, it can steal SMS, call logs, contacts, photos, intercept notifications, stream camera/mic live, and deploy custom phishing overlays targeting banking apps. Its ease of use and subscription-based model lower barriers for attackers, posing serious risks to users especially in BYOD and enterprise mobile contexts.

Attack Type : Mobile RAT

Cause of Issue : Malicious Installer

Industry : Mobile Software

## From Log4j to IIS : Chinese Hackers Reuse Old Bugs for Global Espionage

A China-linked threat actor has revived legacy vulnerabilities including flaws in Log4j, Apache Struts, and Microsoft IIS to target a U.S. non-profit and possibly other institutions. The attackers leveraged multiple old CVEs in a broad scanning effort, then reportedly used credential-based access and DLL side loading for persistence. Their goal appears to be long-term espionage, focusing on domain controllers and sensitive data storage.

Attack Type : Espionage

Cause of Issue : Unpatched Legacy Vulnerabilities

Industry : Enterprise Domain

# Top 5 CVE List

## CVE-2025-42890

A critical flaw allows attackers on the network to abuse built-in, static login secrets and execute remote commands, potentially gaining full database and system control. A fix was released through SAP Note 3666261.

CVSS : 10

Severity : CRITICAL | Attack Type : Remote Code Execution

## CVE-2025-64446

Critical path traversal in FortiWeb by Fortinet allows unauthenticated attackers to bypass auth, create admin accounts, run remote commands, and fully compromise the WAF device.

CVSS : 9.8

Severity : CRITICAL | Attack Type : Remote Code Execution

## CVE-2025-57777

A flaw in Citrix NetScaler ADC and Gateway (when configured as Gateway or AAA server) lets attackers send crafted login requests to leak uninitialized memory, exposing sensitive data like session tokens.

CVSS : 9.3

Severity : CRITICAL | Attack Type : Information Leak

## CVE-2025-62215

A race condition flaw in Microsoft's kernel allows a logged in local attacker to exploit poor synchronization to gain SYSTEM privileges, leading to full machine control.

CVSS : 7.0

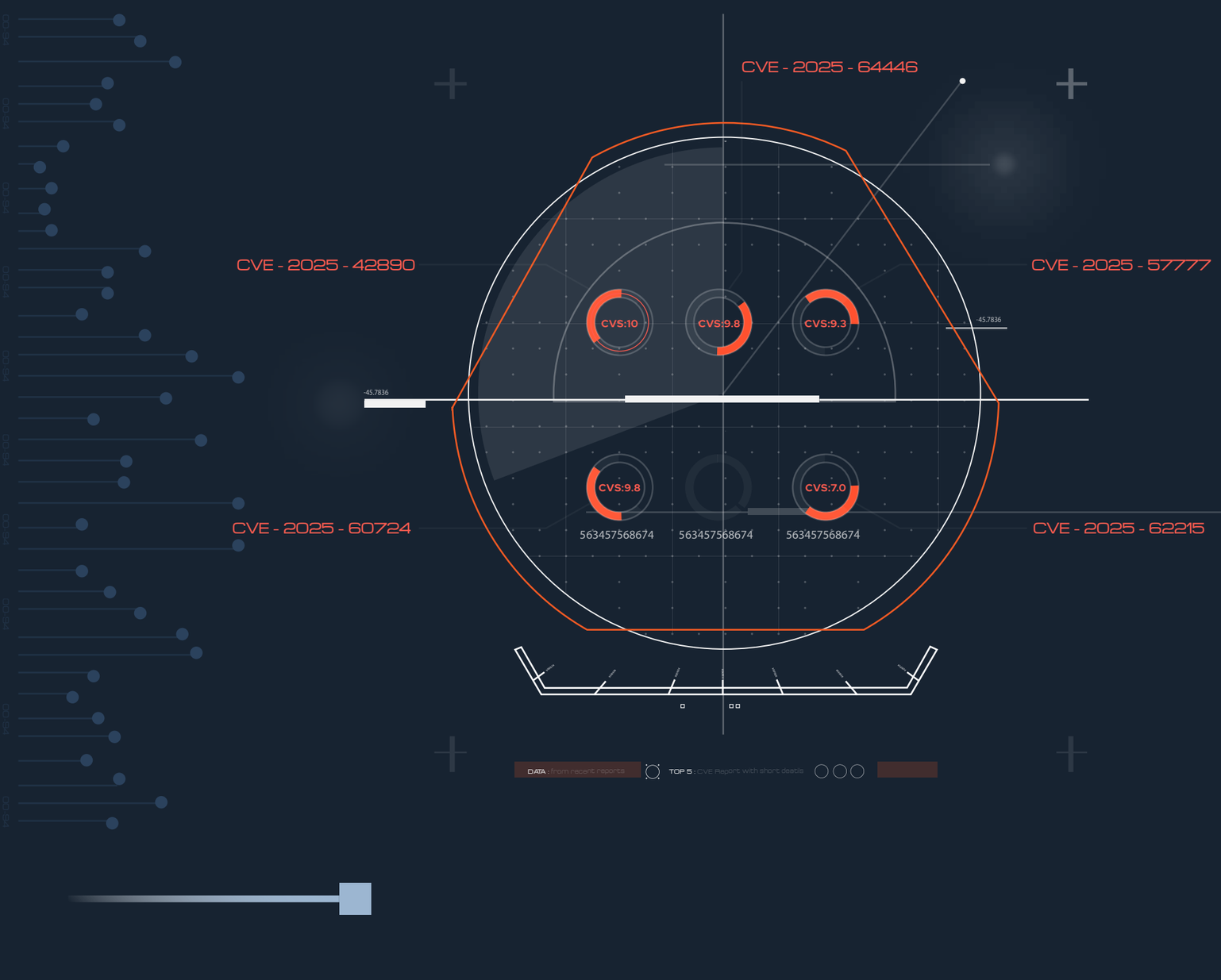
Severity : HIGH | Attack Type : Privilege Escalation

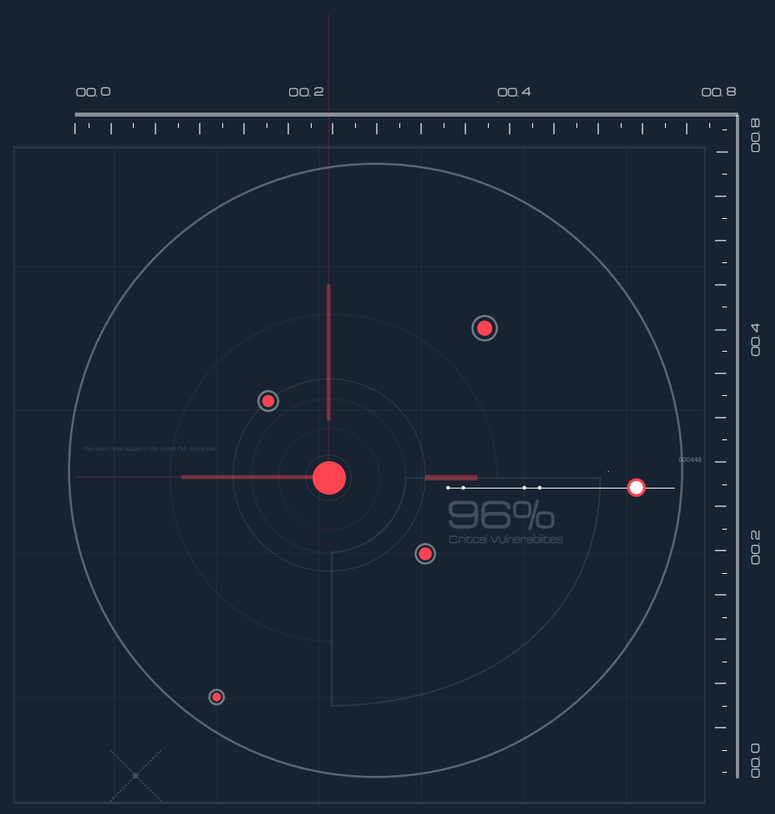
## CVE-2025-60724

Heap-based buffer overflow in Microsoft Graphics Component (GDI+) lets an unauthenticated attacker send a specially crafted document or metafile and trigger remote code execution, leading to full system compromise.

CVSS : 9.8

Severity : CRITICAL | Attack Type : Remote Code Execution




BriskInfosec™
VULNERABILITY TO VICTORY

www.briskinfosec.com

# Top 5 Cybersecurity TV Shows


## Mr. Robot

A realistic thriller about Elliot, a cybersecurity engineer and vigilante hacker, who joins an anarchist group (fsociety) to take down a massive corporation. The show's key lesson is that Social Engineering and Human Error are the most effective vulnerabilities, bypassing even the strongest technical controls.

## Black Mirror

A chilling anthology series exploring the dark, dystopian consequences of near-future tech on society and privacy. A vital caution that new technology is a new attack surface, increasing risks of mass surveillance and data weaponization.

## Person of Interest

A thriller about a former CIA agent and a tech billionaire using an AI surveillance system ("The Machine") to stop crimes. It highlights the security-vs-privacy trade-off inherent in mass surveillance and AI Governance, underscoring the need for encryption.

## Silicon Valley

A hilarious satire of the startup world, following the team at Pied Piper navigating Silicon Valley. The constant battles over code and data underscore the critical importance of intellectual property security and robust infrastructure to business success.

## Halt and Catch Fire

A historical drama set in the 1980s and 90s, chronicling the birth of the personal computer and the internet. It provides crucial context on the foundational security issues and the competitive ethics surrounding the development of Early Code and Network Infrastructure.

BriskInfosec™
VULNERABILITY TO VICTORY

www.briskinfosec.com

*“The strongest security posture starts with the courage to question your own defenses.”*

BriskInfosec™

VULNERABILITY TO VICTORY

+91 44 4352 4537 | +91 73059 79769

contact@briskinfosec.com | www.briskinfosec.com