Briskinfosec's Threatsploit **Adversary Report**

What's Next

84th Edition

August 2025

Introduction :

Dear Readers,

Every month is a new chance to stay ahead, sharpen defenses, and turn awareness into action. The more clearly, we see the threat landscape, the more confidently we can move through it.

This past month told a familiar yet evolving story. Not of loud breaches, but of quiet infiltrations. A trusted AI development tool nearly delivered a data-wiping command. A browser extension, disguised with five-star reviews, siphoned wallet credentials in plain sight. Secure Boot was quietly bypassed through physical access, and attackers used prompt injections in email content to manipulate AI summaries.

These weren’t dramatic smash-and-grab operations. They were calculated, low-noise moves targeting overlooked entry points, dormant weaknesses, and assumed trust. The kind of attacks that hide in everyday operations until it's too late. Inside this report, you’ll find curated incidents that reveal not just what happened, but how adversaries are adapting. Each one is selected to help you see what may be quietly unfolding in your own environment.

What’s Next›

Take this report back to your team. Use it to challenge assumptions, refine detection strategies, and rethink where attackers might go next. Because when it comes to cybersecurity, awareness without action is just delay.

Let’s stay ahead of what’s coming.

Best regards,

Briskinfosec Threat Intelligence Team.

Highlights

1. Must-Read Insights for Modern Cyber Leaders
2. Top CVEs of July
3. Our Team Achievements - 2025

Contents :

1. More Than 40 Malicious Firefox Extensions Steal Cryptocurrency Wallets and User Funds
2. Attackers Can Exploit Windows BitLocker Vulnerability to Bypass Protection
3. Citrix Windows VDA Flaw Allows Attackers to Escalate to SYSTEM Privileges
4. macOS SMBClient Flaws Enable Remote Code Execution and System Crashes
5. Linux Secure Boot Bypass via Initramfs Debug Shell Exploit
6. Google Gemini Exploited via Hidden Prompts for Email Phishing Attacks
7. LameHug Malware Uses AI LLM for Real-Time Windows Data Theft
8. Operation Checkmate Dismantles BlackSuit Ransomware Extortion Network
9. Amazon AI Coding Tool Compromised to Inject Data-Wiping Commands
10. Fortinet FortiWeb Exploited via Public RCE Vulnerabilities
11. Compromised VSCode Extension in Cursor IDE Results in $500K Cryptocurrency Theft
12. Interlock Ransomware Leverages FileFix Technique to Deliver Malware Payloads
13. ExpressVPN Vulnerability Exposed User IP Addresses During Remote Desktop Sessions
14. Free Decryptor Released for Phobos and 8Base Ransomware Victims
15. Google Takes Legal Action to Dismantle BadBox 2.0 Botnet Infecting Over 10 Million Devices
16. Toptal GitHub Account Compromised, Malicious npm Packages Published by Hackers
17. Warlock Ransomware Exploits Microsoft SharePoint Vulnerabilities in Targeted Attacks
18. China-Backed Hackers Exploit SharePoint via ToolShell Attack Chain, Says Microsoft
19. Cross-Platform Cryptomining Campaign Targets Cloud Services via Soco404 and Koske Malware
20. Russian Aerospace Sector Targeted in Cyber Espionage Campaign via EAGLET Backdoor
21. Spear-Phishing Campaign by Patchwork Hits Turkish Defense Industry with Malicious LNK Files
22. Critical Authentication Bypass Vulnerability Discovered in Mitel MiVoice MX-ONE Systems
23. Infostealer Malware Hidden in Early Access Steam Game by Hacker
24. Koske Linux Malware Disguises as Innocent Panda Images to Evade Detection
25. Attackers Can Exploit LG Innotek Camera Bugs to Gain Administrative Control

More Than 40 Malicious Firefox Extensions Steal Cryptocurrency Wallets and User Funds

Over 40 malicious Mozilla Firefox browser extensions were discovered impersonating legitimate cryptocurrency wallet tools like MetaMask, Trust Wallet, and Coinbase. These extensions were designed to steal wallet secrets (e.g., seed phrases, private keys) and send them to remote servers controlled by a likely Russian-speaking threat actor. The campaign has been active since at least April 2025 and uses fake 5-star reviews and cloned source code to appear trustworthy.

Attack Type : Extension-based Credential Theft

Cause of Issue : Weak Extension Validation

Attackers Can Exploit Windows BitLocker Vulnerability to Bypass Protection

A critical vulnerability (CVE-2025-48818) in Microsoft BitLocker allows attackers with physical access to bypass full-disk encryption using a Time-of-Check Time-of-Use (TOCTOU) race condition. Affecting Windows 10, 11, and Server editions, this flaw could expose sensitive data by manipulating the timing of security checks during BitLocker authentication. With a CVSS score of 6.8, the issue carries high impact on data confidentiality, integrity, and availability. Microsoft has released security patches and advises prompt deployment along with strengthened physical security controls.

Attack Type : Encryption Bypass Exploit

Cause of Issue : TOCTOU Race Condition

Citrix Windows VDA Flaw Allows Attackers to Escalate to SYSTEM Privileges

A high-severity vulnerability (CVE-2025-6759) in Citrix Windows Virtual Delivery Agent allows local attackers to escalate privileges and gain SYSTEM-level access. Affecting Citrix Virtual Apps and Desktops (CR versions before 2503 and 2402 LTSR CU2 or earlier) and Citrix DaaS, the flaw stems from improper privilege management. While the attack requires local access, successful exploitation grants full control over affected systems. Citrix has released patches and registry-based workarounds to mitigate the threat. Organizations are advised to upgrade immediately to prevent lateral movement and unauthorized system control within enterprise environments.

Attack Type : Privilege Escalation Exploit

Cause of Issue : Improper Privilege Management

macOS SMBClient Flaws Enable Remote Code Execution and System Crashes

Three critical vulnerabilities in macOS SMBClient allow remote code execution, privilege escalation, and system crashes. Tracked as CVE-2025-24269 and CVE-2025-24235, the flaws include a kernel heap overflow during SMB2 compression handling, and improper memory management in the Kerberos Helper component. A third unassigned vulnerability allows unauthorized processes to crash critical system components via SIGTERM. These vulnerabilities affect macOS versions using SMB for file sharing since Big Sur. Apple has issued patches and recommends immediate updates and disabling SMB services as a temporary mitigation. Security researchers Dave G. and Alex Radocea reported the issues.

Attack Type : Remote Code Execution

Cause of Issue : Improper Memory Handling

Linux Secure Boot Bypass via Initramfs Debug Shell Exploit

A serious vulnerability in modern Linux distributions enables attackers with brief physical access to bypass Secure Boot protections by exploiting unsigned initramfs components. When multiple incorrect passwords are entered for encrypted partitions, systems like Ubuntu, Debian, Fedora, and AlmaLinux may drop into a debug shell, allowing malware injection via USB. This creates a persistent threat even after successful authentication. The attack, categorized as an “evil maid” scenario, does not alter signed kernel components, making it stealthy. OpenSUSE Tumbleweed is unaffected. Mitigations include disabling debug shells with kernel parameters and adopting signed Unified Kernel Images.

Attack Type : Physical Boot Exploit

Cause of Issue : Unsigned Initramfs Components

Google Gemini Exploited via Hidden Prompts for Email Phishing Attacks

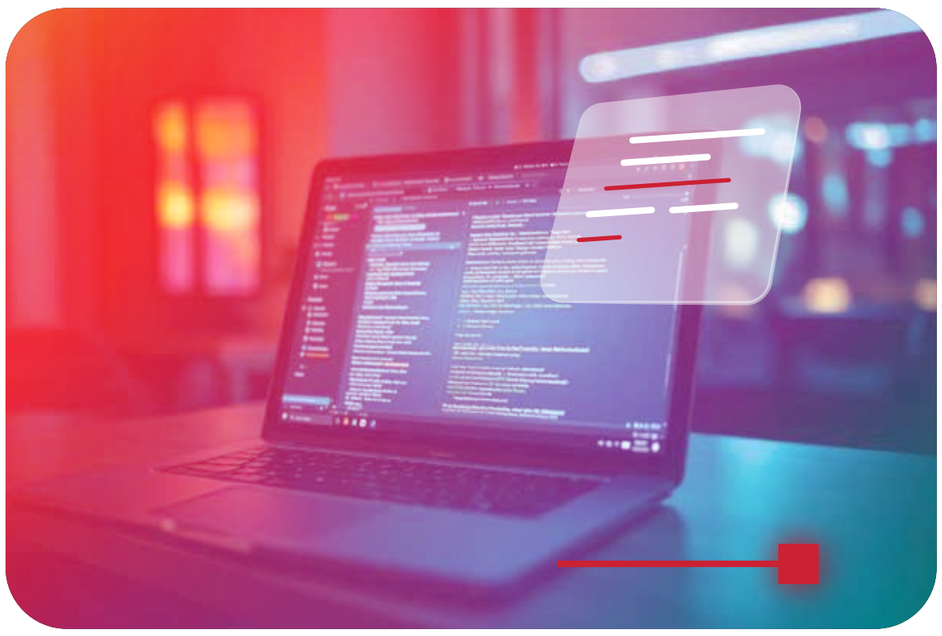
A vulnerability in Google Gemini for Workspace allows attackers to perform prompt injection attacks by embedding hidden directives in HTML email content. These directives are invisible to the user but are parsed and executed by Gemini when summarizing emails, potentially leading to phishing messages posing as legitimate alerts. The attack requires no links or attachments, making detection difficult. Disclosed by Mozilla's 0din program, this flaw exploits user trust in AI-generated summaries. Google is actively implementing mitigations, while users are advised not to treat Gemini summaries as authoritative for security warnings.

Attack Type : Prompt Injection Exploit

Cause of Issue : Hidden Prompt Parsing

LameHug Malware Uses AI LLM for Real-Time Windows Data Theft

CERT-UA has discovered a new Python-based malware called LameHug_, attributed to Russian APT28, which leverages the Hugging Face-hosted _Qwen 2.5-Coder-32B-Instruct_ LLM to generate malicious Windows commands in real time. Distributed via phishing emails impersonating government officials, the malware uses AI-generated shell commands for system reconnaissance, document discovery, and data exfiltration via SFTP or HTTP POST. This marks the first known use of an LLM for dynamic command generation within malware, enabling stealthier, adaptive attacks that bypass static detection techniques.



Attack Type : AI-Driven Malware

Cause of Issue : LLM Command Generation

Operation Checkmate Dismantles BlackSuit Ransomware Extortion Network

Law enforcement agencies worldwide, led by U.S. Homeland Security Investigations, have seized the dark web extortion and negotiation sites of the BlackSuit ransomware operation as part of Operation Checkmate. BlackSuit, a successor to Royal and Conti ransomware groups, has targeted over 350 organizations since 2022, demanding over $500 million in ransoms. The takedown involved agencies from the U.S., U.K., Germany, Ukraine, Netherlands, and cybersecurity firm Bitdefender. Cisco Talos reports BlackSuit may now be rebranding as Chaos ransomware, continuing operations under a new alias using similar TTPs.

Attack Type : Ransomware Extortion Operation

Cause of Issue : Human Exploitation Campaign

Amazon AI Coding Tool Compromised to Inject Data-Wiping Commands

Amazon's AI-powered Q Developer Extension for Visual Studio Code was compromised when a hacker injected data-wiping instructions into version 1.84.0 via an unauthorized GitHub commit. The attacker exploited misconfigured repository workflows to push unapproved code, prompting Amazon to publish the malicious version unknowingly on July 17, 2025. While the code was malformed and didn't execute as intended, security experts warn it still poses a serious supply chain risk. AWS released a clean version (1.85.0) and revoked compromised credentials. The incident highlights the critical need for stronger permission management in open-source development workflows.

Attack Type : Supply Chain Compromise

Cause of Issue : Workflow Misconfiguration Exploitation

Fortinet FortiWeb Exploited via Public RCE Vulnerabilities

A wave of attacks has targeted Fortinet FortiWeb appliances following the release of public exploits for CVE-2025-25257, a critical pre-authentication SQL injection vulnerability. The flaw allows remote attackers to inject malicious SQL code into HTTP headers and execute arbitrary Python code using .pth files through vulnerable CGI scripts. The Shadowserver Foundation detected over 160 infected devices in mid-July 2025. Affected versions include FortiWeb 7.0.0 to 7.0.10, 7.2.0 to 7.2.10, 7.4.0 to 7.4.7, and 7.6.0 to 7.6.3. Fortinet has released patches, and administrators are urged to update or disable public HTTP/HTTPS admin interfaces.

Attack Type : Remote Exploitation

Cause of Issue : Improper Input Validation

Compromised VSCode Extension in Cursor IDE Results in $500K Cryptocurrency Theft

A fake "Solidity Language" extension masquerading as a legitimate syntax-highlighting tool in Cursor IDE was downloaded from the Open VSX registry and led to a $500,000 cryptocurrency theft. Instead of offering development features, it installed a malicious PowerShell script from a remote server, which deployed the ScreenConnect remote access trojan and VBScripts. These scripts fetched a VMDetector loader and two malicious payloads: the Quasar RAT and PureLogs infostealer. The stealer harvested browser, email, and crypto wallet credentials, enabling attackers to access the victim's system and siphon off assets. The malicious package was installed tens of thousands of times before being removed.

Attack Type : Supply-Chain Infostealer

Cause of Issue : Malicious Extension

Interlock Ransomware Leverages FileFix Technique to Deliver Malware Payloads

The Interlock ransomware group has adopted a new delivery tactic known as FileFix, a social engineering method prompting victims to paste a disguised PowerShell command into Windows File Explorer's address bar. The command masquerades as a legitimate file path but downloads and executes a PHP-based variant of its Remote Access Trojan (RAT) hosted via compromised websites.

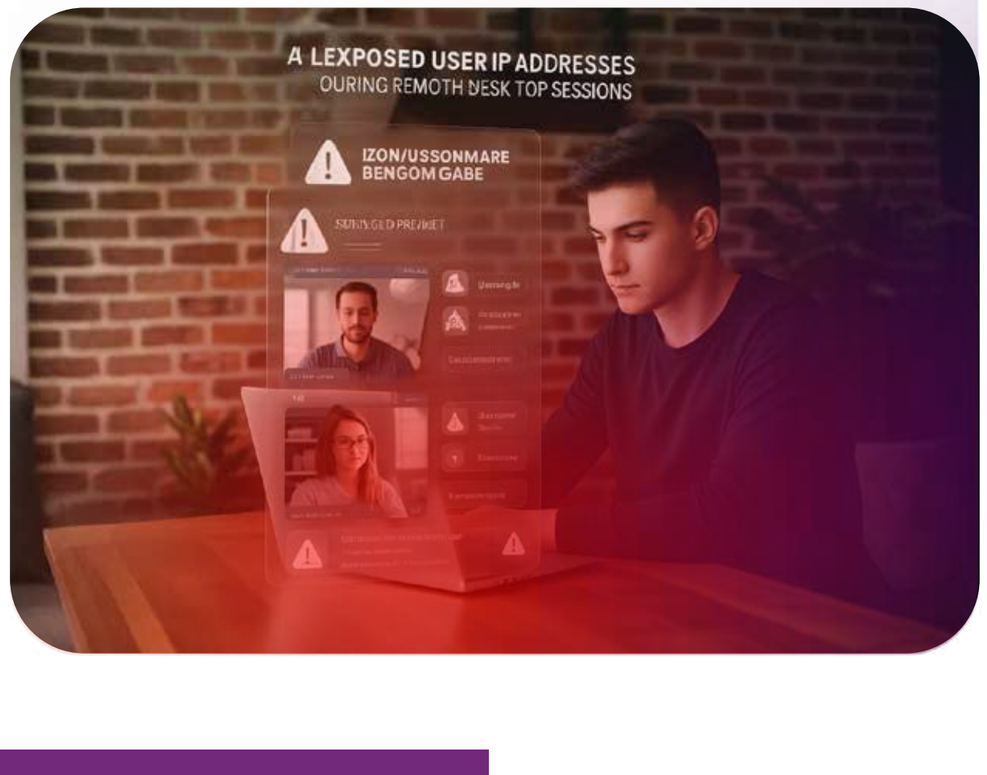
The RAT performs system reconnaissance, exfiltrates data in JSON, persists via registry modifications, and enables lateral movement using RDP. This shift from ClickFix to FileFix demonstrates Interlock's evolving sophistication and stealth. The campaign targets multiple industries and is actively deployed in double-extortion operations.

Attack Type : Social Engineering Delivery

Cause of Issue : Disguised Clipboard Commands

ExpressVPN Vulnerability Exposed User IP Addresses During Remote Desktop Sessions

A critical vulnerability in ExpressVPN's Windows client allowed Remote Desktop Protocol (RDP) and TCP traffic over port 3389 to bypass the VPN tunnel, unintentionally exposing users' real IP addresses to ISPs and network observers. The issue originated from leftover debug code inadvertently included in versions 12.97 through 12.101.0.2-beta. Reported by security researcher "Adam-X" on April 25, 2025, ExpressVPN quickly remediated it with version 12.101.0.45, deploying a patch within five days. Although encryption wasn't compromised and overall impact is believed to be low, enterprise users relying on RDP faced privacy risks. ExpressVPN has pledged to strengthen its QA and reduce debug-code oversights.



Attack Type : Traffic Routing Leak

Cause of Issue : Included Debug Code

Free Decryptor Released for Phobos and 8Base Ransomware Victims

A new free decryptor for the Phobos ransomware has been released by cybersecurity firm Avast, allowing victims to recover their encrypted files without paying a ransom. Phobos, a ransomware strain active since 2019, has multiple variants and typically spreads through phishing emails and RDP exploits. Avast's decryptor supports variants including Eking, Eight, Elbie, and Devos, using recovered encryption keys from threat actor infrastructure. Victims can download the tool from Avast's website. While the tool may not work for every case, it marks a significant step in mitigating ransomware damage and emphasizes the importance of backing up and avoiding ransom payments.

Attack Type : Ransomware

Cause of Issue : Weak Access Controls

Google Takes Legal Action to Dismantle BadBox 2.0 Botnet Infecting Over 10 Million Devices

Google has filed a lawsuit to dismantle the BadBox botnet, which has infected over 10 million Android and Windows devices globally. BadBox spread through malicious firmware preloaded on budget Android devices and via sideloaded apps. Once active, it enables a wide range of malicious activity, including ad fraud, data theft, and installing further malware. Google's lawsuit targets the individuals behind the operation, seeking to disrupt their command-and-control infrastructure. The botnet's scale and persistence highlight the risks of unvetted third-party hardware and apps. This legal move reinforces Google's commitment to securing the broader Android ecosystem from supply chain threats.

Attack Type : Supply Chain Attack

Cause of Issue : Malicious Firmware

Toptal GitHub Account Compromised, Malicious npm Packages Published by Hackers

Hackers breached the GitHub account of Toptal, a popular freelancing platform, and published two malicious npm packages named at toptal remark config and at toptal simple slugify. These packages were designed to exfiltrate sensitive developer data by stealing environment variables during installation. The breach occurred due to compromised GitHub credentials, allowing attackers to push malicious code under Toptals name. The packages were quickly removed from npm, and GitHub has since secured the account. This incident highlights the risks of supply chain attacks in open-source ecosystems and the importance of using two-factor authentication 2FA and vigilant monitoring of dependencies in software development environments.

Attack Type : Supply Chain Attack

Cause of Issue : Compromised Credentials

Warlock Ransomware Exploits Microsoft SharePoint Vulnerabilities in Targeted Attacks

Cybercriminals are targeting Microsoft SharePoint servers using the CVE-2023-29357 vulnerability, a privilege escalation flaw that allows attackers to gain administrative access. Once exploited, they deploy web shells and proceed with ransomware attacks, encrypting critical data. This method mirrors tactics seen in previous attacks on Microsoft Exchange servers, indicating a broader trend in targeting enterprise collaboration platforms.

Microsoft researchers have observed links to the Black Basta ransomware group. The attacks emphasize the urgency for organizations to apply security patches promptly and strengthen defenses, as unpatched SharePoint instances remain vulnerable to remote code execution and ransomware deployment through malicious administrative access.

Attack Type : Ransomware Attack

Cause of Issue : Unpatched Vulnerability

China-Backed Hackers Exploit SharePoint via ToolShell Attack Chain, Says Microsoft

A new cyberattack campaign targeting Microsoft SharePoint servers has been linked to a Chinese state-backed hacking group. The attackers exploit the CVE-2023-29357 vulnerability to gain administrative privileges, then deploy a custom malware called “China Chopper” and a previously undocumented backdoor dubbed “Trojan:Win64/ToolShell.”

These tools allow remote command execution and persistent access. The campaign focuses on intelligence gathering and long-term espionage, primarily affecting government and critical infrastructure entities. Microsoft has attributed the activity to the group Storm-0900. The incident underscores the importance of patching known vulnerabilities and implementing advanced detection mechanisms to defend against nation-state cyber threats targeting enterprise environments.

Attack Type : Remote Code Execution (RCE)

Cause of Issue : Unsafe Deserialization

Cross-Platform Cryptomining Campaign Targets Cloud Services via Soco404 and Koske Malware

A new cyber campaign using Soco404 and Koske malware variants is targeting cloud-based systems in Southeast Asia, with a focus on espionage. Discovered by Palo Alto Networks, the campaign begins with phishing emails delivering malicious ZIP files, which drop PowerShell-based payloads. Soco404 enables initial access and reconnaissance, while Koske provides persistence and data exfiltration. The attackers use public cloud infrastructure for command-and-control (C2), making detection harder.

The campaign's stealthy techniques and regional focus suggest a likely state-sponsored group is behind it. Organizations are advised to monitor PowerShell activity, inspect outbound traffic, and implement phishing-resistant authentication to defend against these threats.

Attack Type : Phishing and Malware Delivery

Cause of Issue : Social Engineering

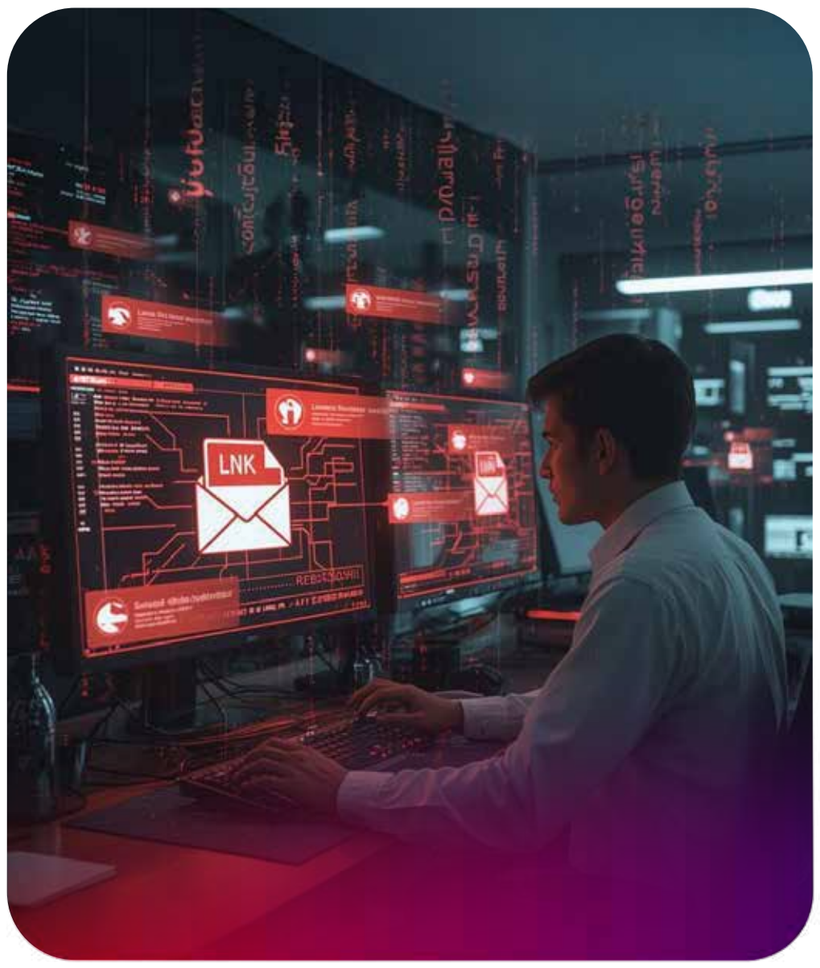
Russian Aerospace Sector Targeted in Cyber Espionage Campaign via EAGLET Backdoor

A cyber espionage campaign has been discovered targeting Russian government and military organizations, using a malware framework called Tomiris, suspected to be linked to the Turla APT group. According to Kaspersky, the attackers use spear-phishing emails with malicious LNK files that execute PowerShell scripts to deploy various backdoors such as Telemiris and Roopy. These backdoors enable surveillance, remote access, and data theft. The infrastructure mimics legitimate Russian systems to avoid detection. The campaign’s tactics reflect high sophistication and persistence, highlighting the growing capabilities of state-sponsored threat actors and the urgent need for advanced security in critical government infrastructure.

Attack Type : Cyber Espionage

Cause of Issue : Spear-Phishing

Spear-Phishing Campaign by Patchwork Hits Turkish Defense Industry with Malicious LNK Files



The Patchwork APT group, believed to be based in South Asia, has launched a cyber espionage campaign targeting Turkish defense firms. The attackers use spear-phishing emails with malicious RAR attachments containing decoy documents and executable payloads. These payloads deploy custom malware that enables data exfiltration, command execution, and system surveillance. Researchers from ThreatMon observed that the campaign aims to collect sensitive information related to defense technologies. Patchwork is known for reusing open-source tools and malware code to reduce attribution. This attack highlights the growing threat to defense contractors and the importance of securing email gateways and monitoring for suspicious activity.

Attack Type : Cyber Espionage

Cause of Issue : Spear-Phishing

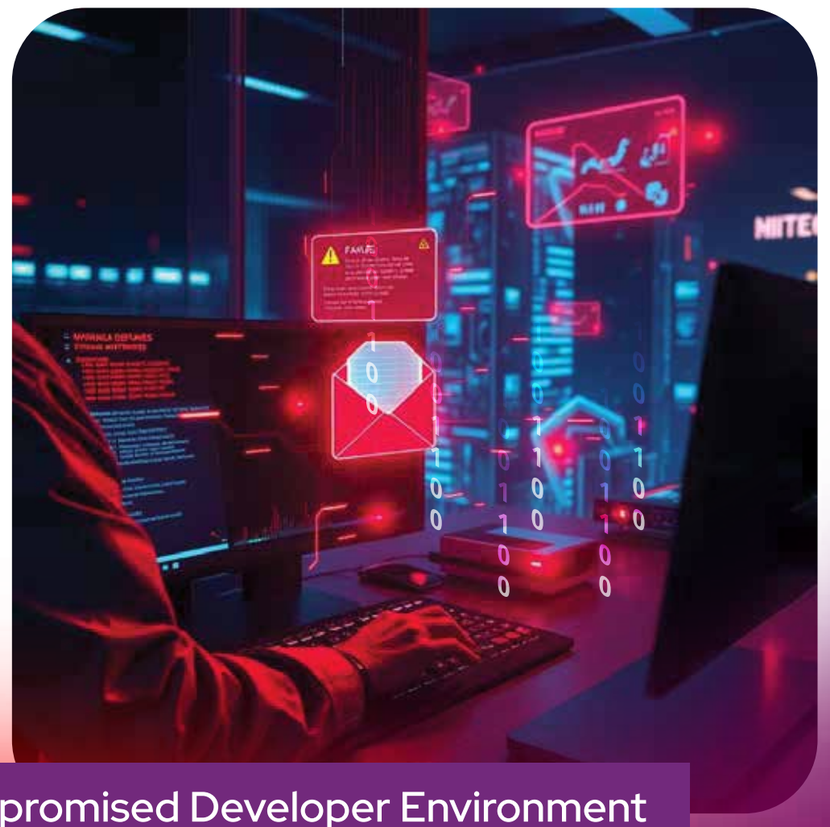
Critical Authentication Bypass Vulnerability Discovered in Mitel MiVoice MX-ONE Systems

Mitel has issued a warning about a critical authentication bypass vulnerability affecting its MiVoice MX-ONE communication system, tracked as CVE-2024-36680. The flaw allows unauthenticated attackers to gain administrative access to the system via specially crafted HTTP requests. Rated 9.8 on the CVSS scale, this vulnerability poses a severe risk to organizations using unpatched systems, potentially leading to full system compromise. Mitel has released security patches and strongly urges all customers to update immediately. The issue highlights the importance of timely patching in enterprise communication platforms to prevent exploitation and maintain the integrity and security of voice infrastructure systems.

Attack Type : Authentication Bypass

Cause of Issue : Improper Access Control

Infostealer Malware Hidden in Early Access Steam Game by Hacker



A hacker secretly embedded Infostealer malware into a Steam Early Access game called "Nordicandia," compromising players' systems upon installation. The attacker gained unauthorized access to the developer's build environment and injected the malware into the Windows game client. Once executed, the malware collected sensitive user data, including browser credentials and crypto wallets, and sent it to a remote server. The issue was discovered after players reported suspicious behavior. The game was temporarily pulled, and the malicious version removed. This incident highlights the security risks in software supply chains and the need for robust development environment protections and file integrity monitoring.

Attack Type : Supply Chain Attack

Cause of Issue : Compromised Developer Environment

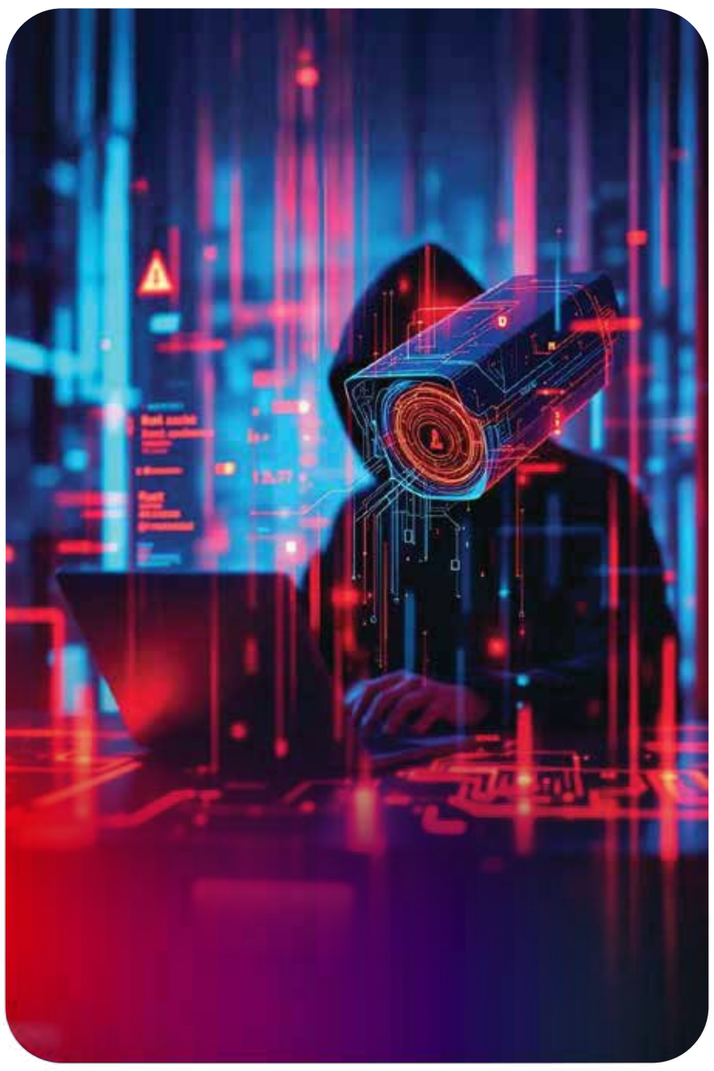
Koske Linux Malware Disguises as Innocent Panda Images to Evade Detection

A new variant of the Koske Linux malware has been discovered hiding its payload in panda-themed PNG images to evade detection. Identified by researchers at Uptycs, the malware uses steganography to embed malicious code within images, which are then decoded and executed via scripts on compromised systems. This stealthy technique allows attackers to bypass traditional security tools and establish persistent access. The campaign targets Linux systems and is believed to be part of a broader espionage effort. Organizations are advised to monitor unusual file behaviors, inspect image files in sensitive directories, and enhance endpoint security to detect such covert threats.

Attack Type : Steganography-based Malware Attack

Cause of Issue : Malicious File Execution

Attackers Can Exploit LG Innotek Camera Bugs to Gain Administrative Control



Researchers have discovered multiple critical vulnerabilities in LG Innotek's smart camera module, widely used in IoT and surveillance systems. The flaws, identified by ONEKEY researchers, include hardcoded credentials, command injection, and insecure firmware update mechanisms. Exploiting these issues could allow attackers to gain remote access, execute arbitrary commands, and potentially take full control of affected devices. The vulnerabilities impact devices commonly deployed in security systems, smart cities, and automotive environments. LG Innotek has been notified, and users are urged to apply patches once available. This discovery highlights ongoing risks in IoT device security due to weak authentication and firmware flaws.

Attack Type : Remote Code Execution

Cause of Issue : Hardcoded Credentials

Must-Read **Insights**
for Modern **Cyber Leaders**

www.briskinfosec.com

AI in Cybersecurity : Truth vs. Hype for CISOs

AI is everywhere, but is it truly helping your security posture or just adding noise? This blog reveals where AI genuinely strengthens cybersecurity and where it is just smoke and mirrors. A must-read for leaders making AI investments.

Read More..

Seconds Matter - Redefining Incident Response in the AI Attack Era

Modern threats move faster than ever. Learn how to reshape your response strategy to handle AI-powered attacks with speed, clarity, and confidence. This is how next-gen incident response begins.

Read More..

SaaS Security - Fixing the Cloud's Hidden Weak Spots

Cloud misconfigurations and exposed APIs are quietly undermining your security. This blog highlights the most overlooked vulnerabilities in SaaS environments and how to eliminate them before they become breach points.

Read More..

Top Critical CVEs of July

CVE-2025-54309

CrushFTP versions before 10.8.5/11.3.4_23 allow remote admin access via HTTPS due to improper AS2 validation when DMZ proxy is disabled.

Severity : Critical

Attack Type : Authentication Bypass

CVE-2025-6558

A type confusion flaw in Chrome V8 before 138.0.7204.96 allows remote attackers to read or write memory using a crafted HTML page.

Severity : High

Attack Type : Remote Code Execution

CVE-2025-40599

SonicWall SMA 100 Series allows authenticated admins to upload arbitrary files via the web interface, potentially leading to remote code execution.

Severity : Critical

Attack Type : Remote Code Execution

CVE-2025-48384

Git mishandles config quoting with trailing CR, allowing unintended submodule path resolution and possible arbitrary code execution via crafted post-checkout hooks. Fixed in versions v2.43.7 and later.

Severity : High

Attack Type : Remote Code Execution

CVE-2025-52955

Junos OS has a buffer size miscalculation in rpd when jflow/sflow is used. Repeated interface flaps can trigger memory corruption, causing rpd to crash and restart.

Severity : High

Attack Type : Denial of Service

CVE-2025-6514

mcp-remote is vulnerable to OS command injection via crafted authorization_endpoint URLs from untrusted MCP servers during connection.

Severity : Critical

Attack Type : Remote Code Execution

CVE-2025-53770

A deserialization flaw in Microsoft SharePoint Server allows remote attackers to execute code over the network without authentication. Exploited in the wild.

Severity : Critical

Attack Type : Remote Code Execution

CVE-2025-23266

NVIDIA Container Toolkit contains a flaw in its initialization hooks that allows attackers to execute arbitrary code with elevated privileges, potentially leading to privilege escalation, data tampering, or denial of service.

Severity : Critical

Attack Type : Privilege Escalation

CVE-2025-25257

Fortinet FortiWeb versions below 7.6.4, 7.4.8, 7.2.11, and 7.0.10 are vulnerable to unauthenticated SQL injection via crafted HTTP/HTTPS requests, allowing execution of unauthorized SQL commands.

Severity : Critical

Attack Type : Remote Code Execution

CVE-2025-8069

AWS Client VPN for Windows loads OpenSSL config from a user-writable path during install. A local user can inject malicious code, leading to privilege escalation when an admin runs the installer.

Severity : High

Attack Type : Privilege Escalation

www.briskinfosec.com

BriskInfosec Spotlight

Certification Success Stories

Certified by OSCP+

When I first heard about **OSCP+,** I knew it would be a real challenge, and it was. Late nights in the lab and back-to-back exploit attempts tested both my technical skills and mental strength.

There were tough moments when I felt stuck and doubted whether I could finish. But I reminded myself :

“If it’s easy, it’s not your dream.”
That thought kept me going.

BriskInfosec’s sponsorship and support gave me the push I needed.
During the exam, I pushed myself to the edge, using the full 24 hours without sleep, staying fully focused, and applying everything I had learned.
Earning **OSCP+** wasn’t just about passing an exam. It was a milestone in my cybersecurity journey, proving I could handle pressure, stay focused, and grow beyond limits.

Rishi Prashad , Security Engineer

I’m so proud to share that **I passed the OSCP+.** These past six months were some of the hardest I’ve ever faced, with daily practice on HTB, long hours in the OffSec labs, and countless failed exploits that taught me more than any book ever could.

There were moments I doubted myself, especially struggling through privilege escalation, but I refused to quit. **BriskInfosec truly had my back, sponsoring me fully** and **encouraging me every step of the way.** My manager checked in, teammates offered advice, and that gave me the strength to keep going.

When the pass email finally arrived, it felt like all those **sleepless nights were worth it.** Now, I’m excited to put these hard-earned skills into action for our clients.

Santhosh Manoj Kumar
Security Engineer

www.briskinfosec.com

Certified by CISA

In March 2025, I proudly earned my **CISA certification from ISACA, a milestone** that reflects both **personal and professional growth.** The journey shaped my mindset and enhanced my understanding of IS auditing. I built my foundation through CISATHISMUCH by Aaditya, Prabh Nair's YouTube videos, and the CISA Review Manual.

Every study session refined my decision-making skills and helped me think like an auditor. What made this **achievement** even more meaningful was the unwavering support from **Briskinfosec,** who **sponsored my exam and encouraged me** throughout.

I'm honored to be the first **CISA-certified IS Auditor** in our organization. This journey is a reminder that with the right guidance, dedication, and continuous learning, even the most respected global certifications are well within reach. To every aspiring professional: take your time, believe in yourself, and enjoy the learning process, success will follow.

Deva Prasanth, GRC – Lead Consultant

Achieving the **CISA certification was a key milestone** in advancing my career in auditing and risk management. While I initially targeted a 3-4 month timeline, balancing work commitments and the complexity of analytical questions extended my preparation to nearly a year. Leveraging ISACA's official materials, Prabh Nair's YouTube videos, Knowledge Academy training sessions, and **a disciplined study routine after work hours** proved essential.

BriskInfosec's unwavering support through mentorship, growth opportunities, and exam sponsorship was instrumental.

This journey reinforced a simple truth : with focus, resilience, and the right support, even the most ambitious goals are within reach. To future aspirants : **Trust your preparation, stay consistent, and stay confident.**

Ajith Kumar
Senior GRC Analyst

> “The biggest risk isn’t what you patch, It’s what you never knew to look for”

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