Threatsploit
Adversary Report

Edition - 87 | November 2025

$4.9M
The average cost of a phishing breach

91%
Cyberattacks start with a phishing email

1/5
Still click suspicious emails

88%
Breaches stem from simple human errors

10min
Attackers breach systems

52%
Phishing emails use AI deception

BriskInfosec
VULNERABILITY TO VICTORY

www.briskinfosec.com

Dear Readers

Every headline may reveal an attack, but few reveal the pattern behind it. Our Adversary Report continues to serve as a lens into the pulse of the global threat ecosystem. Each month, as adversaries refine their tradecraft, this report helps leaders connect the unseen dots, showing how one breach connects to another, how a single exploit can ripple across industries, and how unseen links shape the bigger threat picture.

This month, the digital battlefield witnessed an alarming escalation. The LockBit, Qilin, and DragonForce alliance signals a new phase of coordinated ransomware campaigns, where threat groups are joining forces like business partners. Meanwhile, the MatrixPDF toolkit weaponized everyday documents into phishing payloads, and Android's VNC exploit opened fresh doors to mobile compromise.

The turbulence did not stop there. The Renault and Dacia UK breach exposed sensitive data through third-party compromise, while the Rhadamanthys Stealer's new fingerprinting capability showed how malware now studies its victims before striking. Add to that CVE-2025-10547 and CVE-2025-61882, both actively exploited, and it becomes clear that the real danger lies not in what is new but in what is left unattended.

As you turn these pages, reflect on the changing rhythm of cyber conflict. The patterns you see here are more than incidents; they are signals of what is shaping tomorrow's security landscape. Staying ahead begins with understanding, and understanding begins here.

Best Regards

Briskinfosec Threat Intelligence Team

CRAC-KED IN-SIGHTS

- Every click counts
- Before the Next Breach , Know your Cyber Health
- Top CVE’s of October 2025

01

Cyber Cartels on the Rise

Powerful ransomware groups like LockBit, Qilin, and DragonForce are joining forces, creating global extortion networks targeting critical systems. Even trusted tools like Velociraptor are being twisted into ransomware enablers.

02

Smarter Attacks, Smarter Defenses

AI is now both the attacker and the shield, Russia deploys AI-powered phishing, while Google and Apple boost AI bug-bounty defenses. The rise of AI agents also brings new data-leak challenges.

03

Trust Breached, Data Exposed

Massive leaks hit Renault, SonicWall, and Framework Laptops, exposing sensitive data through cloud misconfigurations and insecure backups, proving that no industry is immune from data compromise.

04

Exploiting the Invisible Flaws

Attackers exploited bugs in DrayTek routers, Redis, Unity Engine, and Oracle systems, highlighting how unpatched software remains a silent gateway to global exploitation.

05

Deception in Every Download

From MatrixPDF's weaponized documents to Klopatra's mobile control and fake job offers by Lazarus Group, cybercriminals are mastering manipulation to steal data and access devices.

06

Securing the Digital Frontier

Organizations are urged to shift focus.Google Workspace pushes target-centric defense, while experts stress AI governance, MFA, and zero-trust policies to stay ahead of the threat curve.

LockBit Qilin DragonForce Form Deadly Ransomware Cartel Escalation Imminent!

Three ransomware giants; LockBit, Qilin, DragonForce forge a cartel, pooling tech, affiliates, and tools for amplified global extortion. This unholy alliance accelerates attacks on critical infrastructure, merging data theft, encryption, and double-extortion for unprecedented scale and speed.

Attack Type : Ransomware | Cause: Coordinated Threat Alliance | Industry: IT

Takeaways : Monitor affiliate networks; deploy multi-layered defenses and share threat intel across sectors.

MatrixPDF Turns PDFs into Deadly Phishing Traps Bypassing All Filters!

MatrixPDF toolkit weaponizes PDFs with blurred text, fake secure prompts, overlays, and JS redirects to phishing or malware sites. It evades email scanners like Gmail by using external links, tricking users into credential theft or infections.

Attack Type : PDF Phishing | Cause: Malicious PDF Toolkit | Industry: IT

Takeaways : Scan PDFs with advanced tools, train users on suspicious docs and enable email sandboxing.

Google Drive AI Detects Ransomware Onslaught Saves Files from Cloud Catastrophe!

Google Drive desktop rolls out AI that spots ransomware by monitoring sync for mass encryption, pausing uploads and alerting users. Trained on real samples, it prevents cloud propagation and enables quick restores, averting widespread data loss.

Attack Type : Ransomware | Cause: Ransomware Infection | Industry: IT

Takeaways : Integrate AI monitoring in cloud tools; test restores and update sync policies regularly.

Klopatra Android Malware Grants Full VNC Control Over Your Device!

Klopatra malware poses as IPTV/VPN apps, infecting 3000+ European devices to enable silent VNC for real-time control even screen off. Attackers steal creds, keystrokes, and execute fraud, crippling mobile security.

Attack Type : RAT | Cause: Malicious App Distribution | Industry: Telecommunications

Takeaways : Vet apps from trusted sources; deploy mobile EDR and restrict sideloading.

Renault Dacia UK Data Breach Exposes Customer Secrets to Phishers!

Hackers breach third-party provider, stealing names, contacts, vehicle data from Renault/Dacia UK customers; no finances hit. This fuels phishing scams, eroding trust and risking identity theft.

Attack Type : Data Breach | Cause: Third-Party Compromise | Industry: Automotive

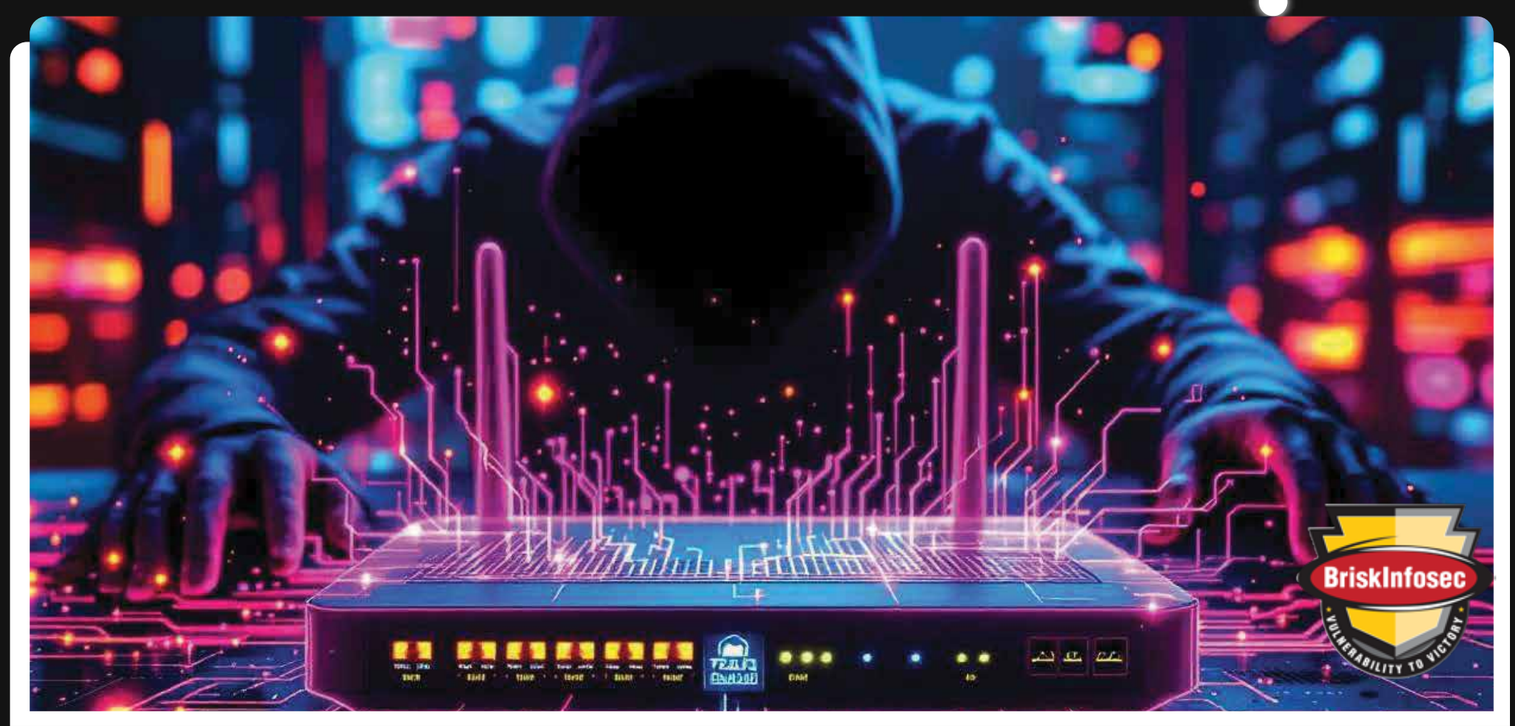
Takeaways : Audit third-party access; enforce MFA and monitor for phishing spikes.

DrayTek Routers RCE Flaw Lets Hackers Commandeer Networks Remotely!

CVE-2025-10547 in DrayTek Vigor routers allows unauth RCE via crafted HTTP requests, giving attackers a remote entry point. Successful exploitation triggers memory corruption, which attackers can abuse to gain full control of affected devices. With device control, adversaries can pivot inside networks, bypassing perimeter defenses and moving laterally. Sensitive assets such as data, credentials, and network configurations become exposed to theft or tampering.

Attack Type : RCE | Cause: Uninitialized Variable Vulnerability | Industry: Telecommunications

Takeaways : Patch routers immediately; segment networks and log HTTP anomalies.



Rhadamanthys Stealer Evolves with Fingerprinting PNG Hides Payload Doom!

Rhadamanthys 0.9.2 adds device fingerprinting to dodge sandboxes and PNG steganography to conceal payloads in images. This steals creds, evades detection, and persists in infections.

Attack Type : Information Stealer | Cause: Malware Infection | Industry: IT

Takeaways : Scan images for steganography; enable fingerprinting detection in EDR.

BatShadow Vampire Bot Lures Job Seekers into Go Malware Nightmare!

BatShadow uses fake job ZIPs with PDFs/executables to deploy Vampire Bot, profiling systems, capturing screens, and exfiltrating data via C2. This targets HR, stealing sensitive info.

Attack Type : Malware | Cause: Malicious Email Attachment | Industry: Human Resources

Takeaways : Block suspicious attachments; train on job scam awareness.

Storm-1175 Medusa Ransomware Ravages GoAnywhere Victims Worldwide!

Storm-1175 exploits CVE-2025-10035 in GoAnywhere MFT to achieve remote code execution, providing initial access to victim environments. Once inside, the threat actor deploys Medusa to encrypt sensitive files and establish persistent exfiltration channels. Encrypted and exfiltrated data are then leveraged for extortion, disrupting business operations and jeopardizing customer trust. Enterprises should prioritize incident response readiness, immediate patching, and outbound data monitoring to limit impact.

Attack Type : Ransomware | Cause: Vulnerability Exploitation | Industry: IT

Takeaways : Patch file transfer tools; monitor for RCE indicators.

Cl0p Exploits Oracle EBS Flaw for Mass Ransomware Assault!

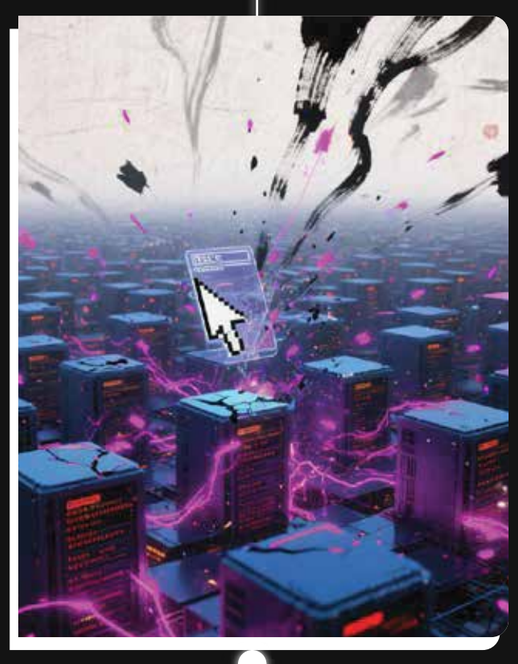
Cl0p hits Oracle EBS with CVE-2025-61882 for unauth RCE, deploying ransomware since August, stealing data from exposed instances. This causes widespread encryption and leaks.

Attack Type : RCE

Cause: Unpatched Software Vulnerability

Industry: IT

Takeaways : Update Oracle suites; restrict public exposure.



Redis Critical Flaw Enables RCE on Thousands of Exposed Instances!

CVE-2025-49844 in Redis Lua allows auth RCE, spawning shells on exposed instances lacking auth. This leads to full compromise and pivots.

Attack Type : RCE

Cause: Improper Memory Management

Industry: IT

Takeaways : Secure Redis with auth; patch Lua components urgently.

Unity Engine Bug Exposes Gamers to RCE Privilege Escalation Chaos!

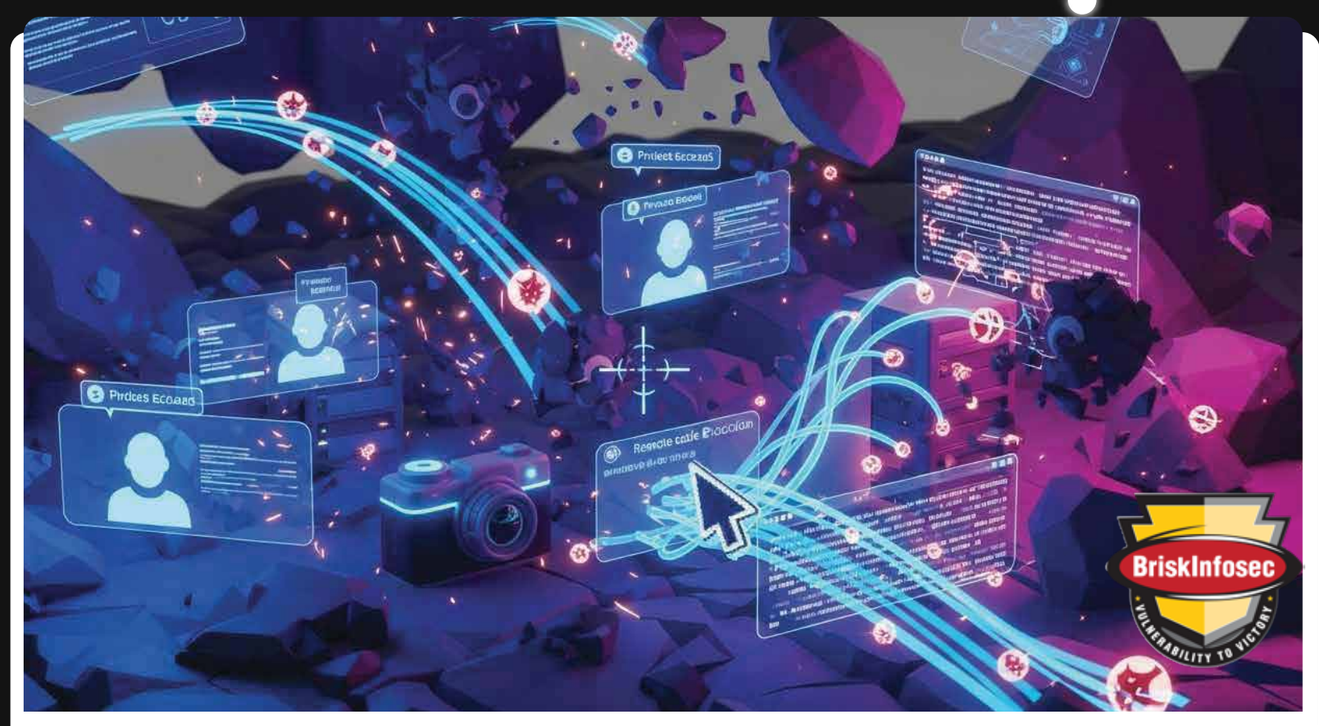
CVE-2025-59489 in Unity allows RCE and privilege escalation via unsafe file inclusion in Android and Windows apps. Attackers can craft or supply malicious files that games load, enabling arbitrary code execution inside the app. Compromised games may deliver malware, steal credentials, or escalate privileges on affected devices. Millions of users are at risk—developers must patch, validate file inputs, and adopt secure file-loading practices.

Attack Type : RCE

Cause : Unsafe File Handling

Industry: IT

Takeaways : Rebuild Unity apps; scan for vulnerable games.



Every Click Counts

One careless click can trigger an entire cyberattack chain

$4.9M
The average cost of a phishing breach

91%
Cyberattacks start with a phishing email

1/5
Still click suspicious emails

88%
Breaches stem from simple human errors

10min
Attackers breach systems

52%
Phishing emails use AI deception

Technology can filter millions of threats but it can’t stop one careless click.

BriskInfosec
VULNERABILITY TO VICTORY

Kido Nursery Breach Doxing 8000 Kids Teens Arrested in Extortion Horror!

Radiant Group ransomware hits Kido nursery chain, encrypting systems and doxing personal data of 8,000+ children online. Teens exploit leaked info for blackmail; parents panic as addresses and photos spread on dark web. London police arrest suspects, shows how child data fuels real-world harm.

Attack Type : Ransomware | Cause: Unauthorized Access | Industry: Education

Takeaways : Encrypt all PII at rest; isolate student data and enable dark web monitoring.

Protect Targets Not Perimeters Modern Google Workspace Defense Urgent!

Attackers abuse OAuth in Google Workspace to silently access Drive, Gmail, and Meet without MFA prompts. Once inside, they exfiltrate contracts and IP, perimeter tools fail. Shift to identity-centric defense is now mandatory.

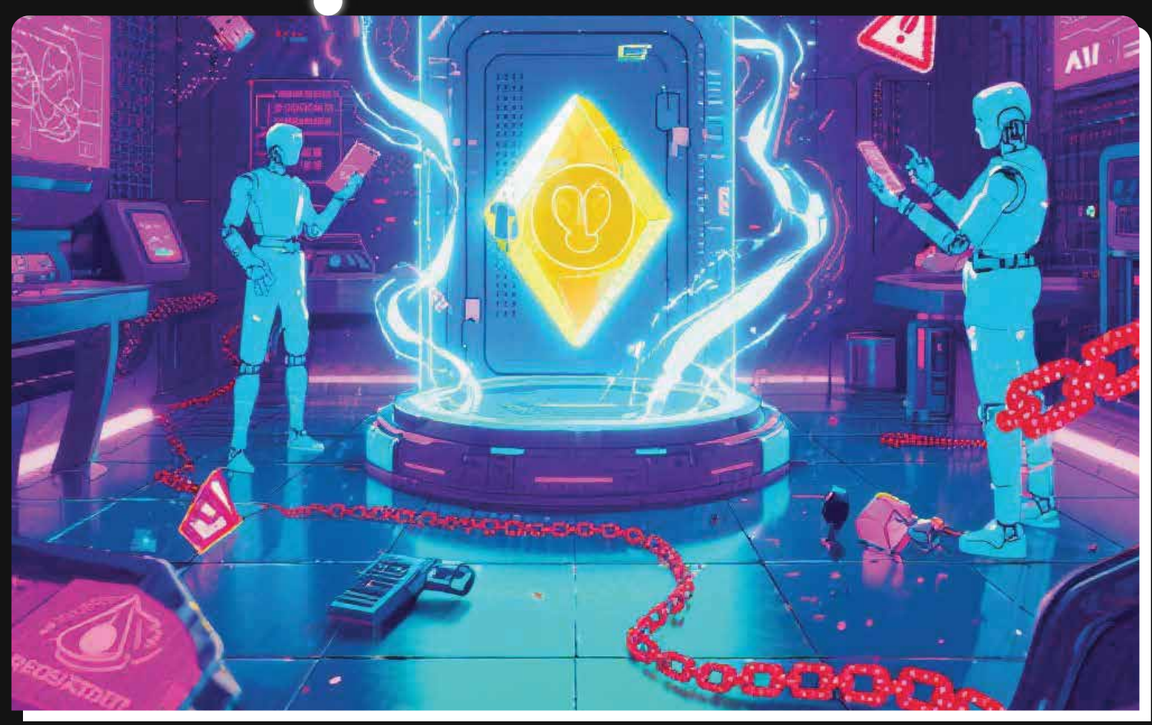
Attack Type : Account Compromise | Cause: OAuth Token Abuse | Industry: IT

Takeaways : Inventory all OAuth apps weekly; enforce context-aware access and token binding.

Google AI Bug Bounty Hits $2M for Zero-Click RCE Discoveries!

Google offers $2M for zero-click RCE in Gemini and AI APIs, flaws allow remote code without user action. State actors and ransomware groups race to weaponize AI platforms. A single exploit could hijack millions of AI workflows.

Attack Type : RCE | Cause : Design Flaws | Industry: Artificial Intelligence



Takeaways : Participate in AI bug bounties; sandbox all LLM outputs and isolate AI runtimes.

SonicWall Cloud Firewall Backups Stolen Credentials Rules Exposed!

Hackers breach SonicWall's cloud backup portal, stealing encrypted configs, VPN certs, and firewall rules. Though networks stayed up, leaked rules enable surgical bypass attacks. Full credential reset now urgent.

Attack Type : Data Breach

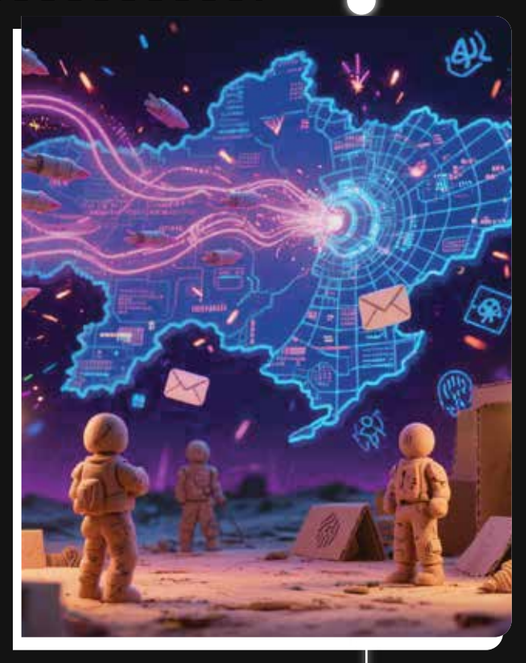
Cause: Compromised Cloud Backups

Industry: Networking

Takeaways : Rotate all firewall certs post-incident; store backups offline with air-gapped access.

Russia Wields AI in Ukraine Cyber War Phishing Malware Rampage!

Russia deploys AI to generate hyper-realistic phishing emails and deepfake video calls targeting Ukrainian officials. Over 3,000 incidents in 90 days, bypasses all traditional filters. Hybrid warfare now runs on generative AI.



Attack Type : Phishing

Cause: AI-Enhanced Operations

Industry: Government

Takeaways : Deploy AI-based email anomaly detection; train staff on deepfake verification protocols.

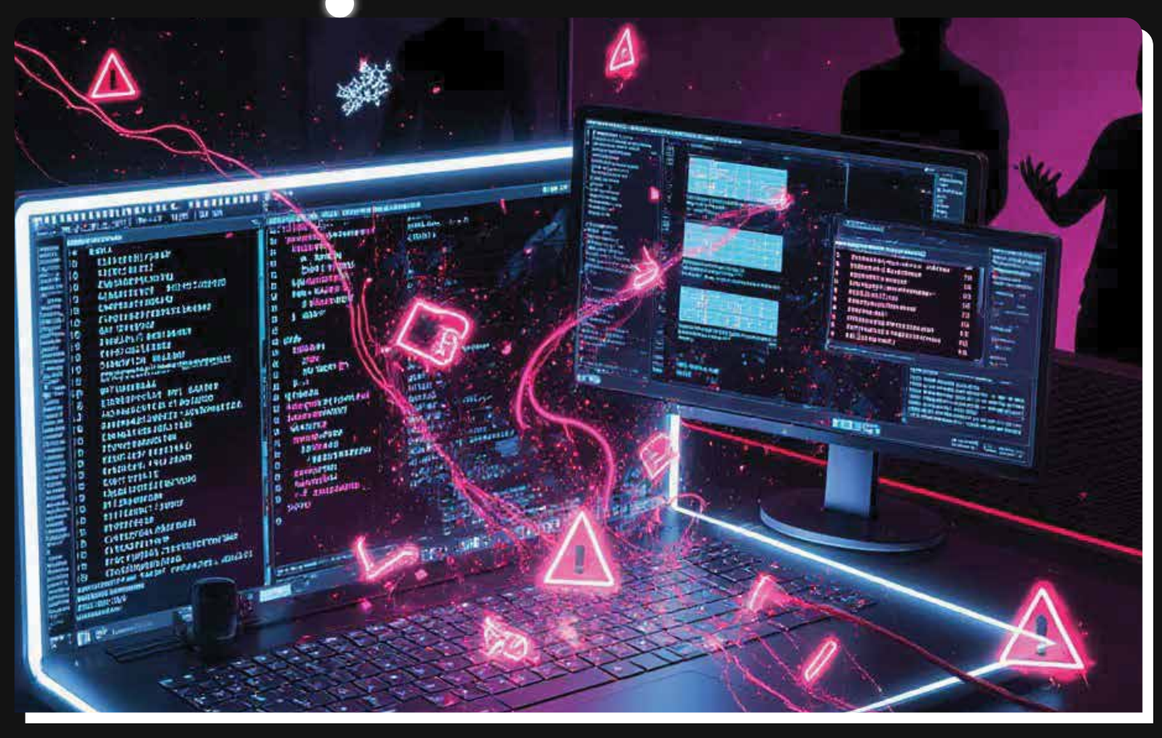
Velociraptor DFIR Tool Twisted into Ransomware Enabler by Hackers!

Hackers chain CVE-2025-6264 in old Velociraptor with SharePoint RCE to deploy LockBit and Babuk. Forensics tool becomes persistence engine — ironic and deadly. SOC teams now scan their own tools.

Attack Type : Ransomware

Cause : Outdated DFIR Tool

Industry: IT



Takeaways : Audit and update all DFIR agents; block unsigned binaries in security workflows.

Stealit Malware Hides in Node.js Installers Steals Wallets Secrets!

Stealit hides in cracked game and VPN installers using Node.js single-file executables to harvest Discord tokens, browser passwords, and crypto wallets. Over 50,000 infections via torrent sites. Devs and gamers hit hardest.

Attack Type : Info Stealer

Cause: Bundled Installers

Industry: Software Distribution

Takeaways : : Scan all downloaded executables; avoid cracked software and use official repos only.

Payroll Pirates Storm-2657 Hijack HR Accounts Divert Salaries!

Storm-2657 phishes HR teams in Workday and BambooHR, using MFA fatigue to approve salary reroutes. $1.2M diverted from schools and nonprofits in 60 days. Payroll fraud now fully automated.

Attack Type : Account Takeover

Cause: HR SaaS Compromise

Industry: Human Resources

Takeaways : Enable hardware keys for HR logins; require dual approval for payment changes.

PhantomCaptcha Targets Ukraine Aid with Fake Zoom RAT Onslaught!

PhantomCaptcha sends fake Zoom invites with trojanized PDFs to Red Cross and UNICEF staff. MISTPEN RAT deploys on click, exfiltrates donor lists and aid routes. Humanitarian ops now under cyber siege.

Attack Type : RAT

Cause : Fake Zoom PDFs

Industry: Government

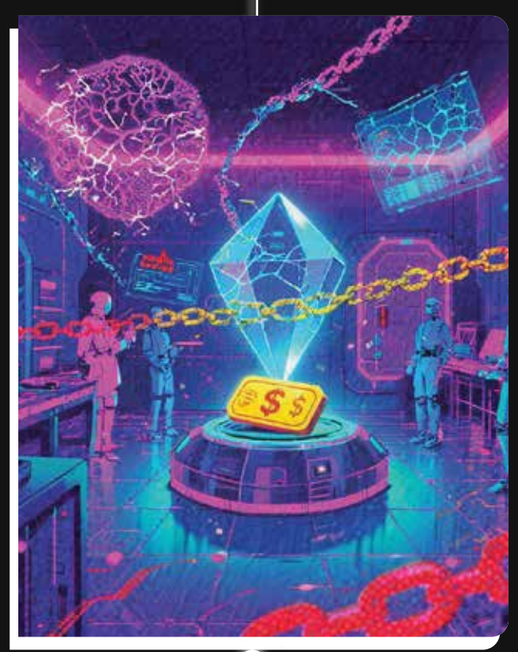
Takeaways : Block executable PDFs; verify all meeting links via official channels.

Massive Botnet Hammers US RDP with Enumeration Attacks Worldwide!

100k+ botnet IPs from 100 countries probe US RDP servers for valid usernames via timing attacks. Precursor to credential stuffing — average org faces 40k attempts daily. Lockout policies failing.

Attack Type : Brute Force | Cause: Weak Credentials | Industry: IT

Takeaways : Disable RDP externally; enforce allow-lists and fail2ban with geo 3-strike rules.



Apple $2M Bounty for Zero-Click RCE Flaws Platform Integrity at Stake!

Apple raises bounty to $2M for zero-click RCE in iOS/macOS kernel, exploits survive reboots and updates. Used by spyware vendors; one flaw = total device control. Platform trust hangs by a thread.

Attack Type : RCE | Cause: Design Flaw | Industry: Mobile Platforms

Takeaways : Keep devices on latest patch; enable Lockdown Mode for high-risk users.

Malicious VSCode Extensions Steal Crypto Wallets on OpenVSX Again!

Fake VSCode extensions on the OpenVSX registry contained malicious code that injected wallet drainers into developer environments. Over 1,200 downloads happened before removal, giving attackers a sizable window to compromise Solidity and Rust developers. Infected developer machines can leak private keys, manipulate source code, or introduce further backdoors into projects. This shows IDEs and open-source registries are critical supply-chain attack vectors — teams must vet extensions, monitor dependencies, and restrict privileged secrets in development environments.

Attack Type : Crypto Malware | Cause: Malicious Extensions | Industry: IT

Takeaways : Only install from Microsoft Marketplace; enable extension signature verification.

Before
the Next Breach

-Know Your Cyber Health.

Scan the QR code
to get your objective score.

BriskInfosec
VULNERABILITY TO VICTORY

AI Agents in Teams Unleash Data Leaks Privilege Abuse Risks!

Unmanaged AI agents in Microsoft Teams read internal chats, files, and meetings, some auto-exfiltrate to external APIs. One rogue agent = full data breach. AI scale now outpaces governance.

Attack Type : Data Exposure

Cause: AI Agent Access

Industry: IT

Takeaways : Create AI agent allow-lists; log and audit all agent data access in real time.

Framework Laptops Secure Boot Flaw Opens Door to Persistent Bootkits!

Signed UEFI diagnostic shell in 200k Framework laptops allows memory writes to disable Secure Boot. BlackLotus and Bootkitty now persist through OS wipes. Physical access not required.

Attack Type : Bootkit

Cause: Unsafe UEFI Shell

Industry: Hardware

Takeaways : Apply Framework's BIOS fix; verify Secure Boot state on every boot.

Chinese Flax Typhoon Turns ArcGIS into Year-Long Backdoor Nightmare!

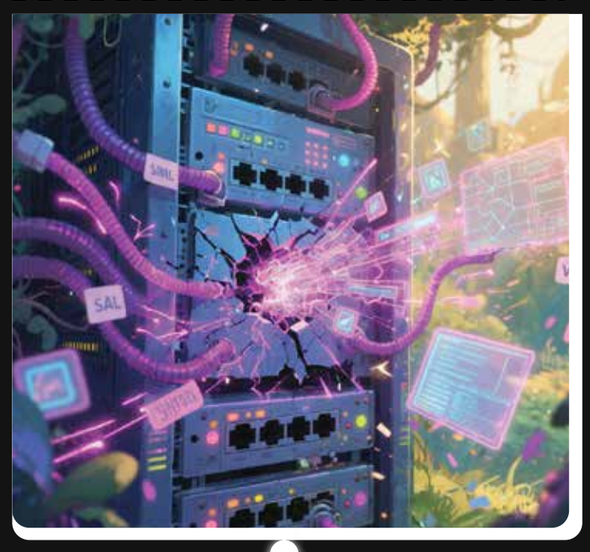
Flax Typhoon (China) compromises public ArcGIS servers and converts them into web shells using a hardcoded key, providing stealthy remote access. The group maintained persistence for over 14 months, enabling prolonged reconnaissance and data collection across victim networks. They deploy a VPN bridge from the compromised GIS server to pivot internally, facilitating lateral movement and access to sensitive systems. Geospatial systems become silent C2 hubs, organisations must audit public-facing GIS services, rotate keys, and monitor for anomalous VPN and web-shell activity.

Attack Type : Persistent Access

Cause: Server Exposure

Industry: Geospatial

Takeaways : Harden public-facing GIS servers; monitor for unauthorized SOE modifications.



Cisco SNMP Exploit Deploys Rootkit on Switches VLAN Lateral Havoc!

Operation Zero Disco uses CVE-2025-20352 + old CMP flaw to install fileless rootkit on Cisco 9300/9400 switches. Bypasses logs, crosses VLANs, survives reboot. Network core = compromised.

Attack Type : RCE

Cause: SNMP Vulnerability

Industry: Networking

Takeaways : Disable SNMPv2; enable SNMPv3 with ACLs and inspect switch firmware.

North Korean Lazarus Fake Jobs Steal Drone Secrets from Engineers!

Lazarus runs “Operation Dream Job” since March 2025, fake recruiter emails with PDF résumés deploy MISTPEN RAT. Steals UAV blueprints from European defense firms. NK drone program accelerates.

Attack Type : Social Engineering

Cause: Trojanized Docs

Industry: Defense

Takeaways : Train engineers on recruitment scams; sandbox all job-related attachments.

Secure AI Webinar Exposes Unmanaged Agents as Massive Backdoors!

AI agents now outnumber employees 3:1 in large firms, most lack identity controls. One compromised agent = full network access. Webinar urges zero-trust for AI. Future attacks will be agent-led.

Attack Type : Data Exposure

Cause : Unmanaged AI

Industry: IT

Takeaways : Assign unique identities to AI agents; enforce least-privilege and auto-revoke.

Top 5
CVE's Of October 2025

Severity : Critical

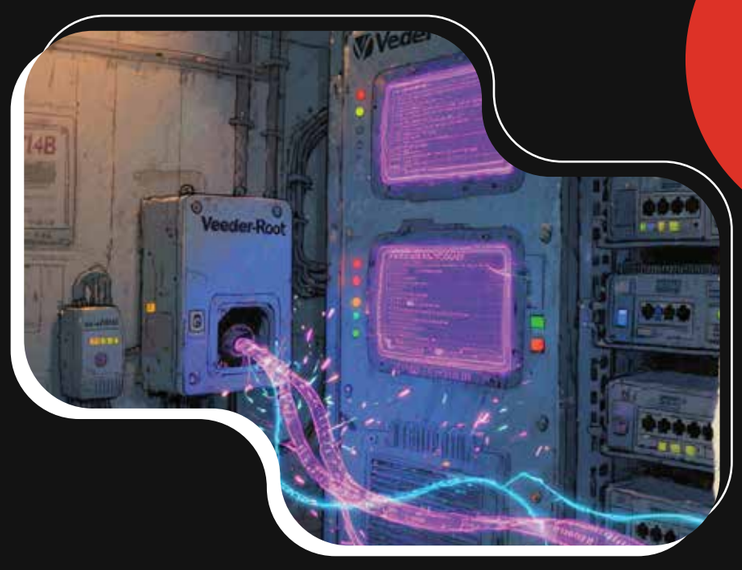
CVE-2025-59287

Deserialization flaw in Windows Server Update Services enabling unauthenticated remote code execution with SYSTEM privileges via crafted AuthorizationCookie objects.

Attack Type : Remote Code Execution

CVSS Score
9.8

CVSS Score
9.4



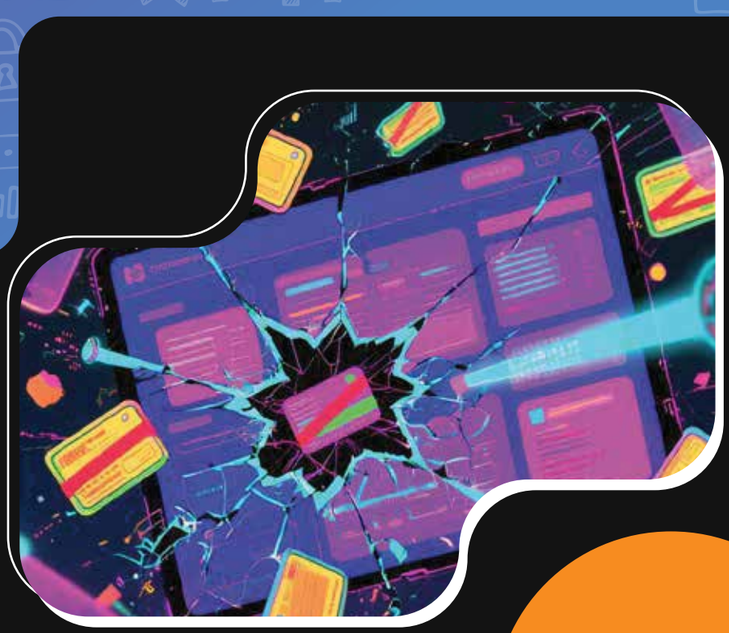
Severity : Critical

CVE-2025-58428

Command-injection in Veeder-Root TLS4B (SOAP) lets authenticated attackers run arbitrary Linux commands, get shell access move laterally in ICS/infra.

Attack Type : Code Execution

Severity : High



CVE-2025-61884

Unauthenticated flaw in Oracle E-Business Suite allows attackers to access sensitive business data via exposed runtime UI, causing info disclosure.

Attack Type : Information Leak

CVSS Score
7.5

BriskInfosec
VULNERABILITY TO VICTORY

Severity : Critical

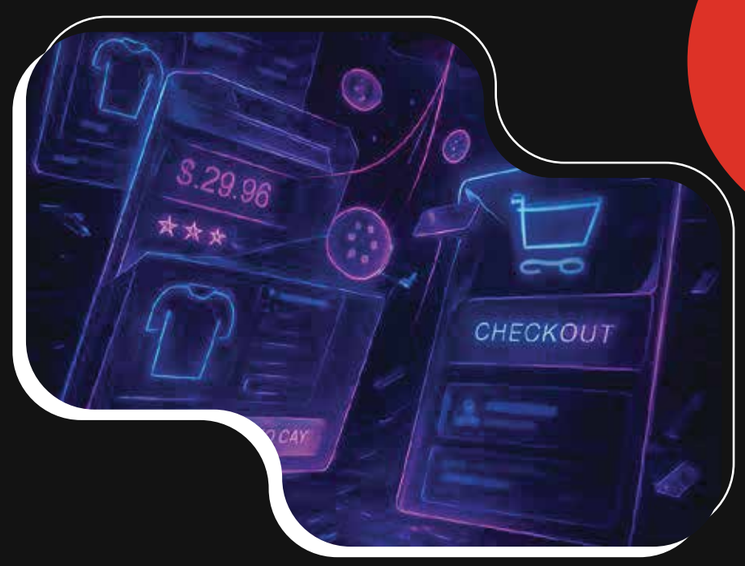
CVE-2025-61932

Improper origin validation in LANSCOPE Endpoint Manager allows remote attackers to execute arbitrary code on endpoints without authentication.

Attack Type : Remote Code Execution

CVSS Score

9.3



CVSS Score

9.1

Severity : Critical

CVE-2025-54236

Improper input validation in Adobe Commerce/Magento lets unauthenticated attackers hijack user sessions and potentially execute remote code.

Attack Type : Bypass

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