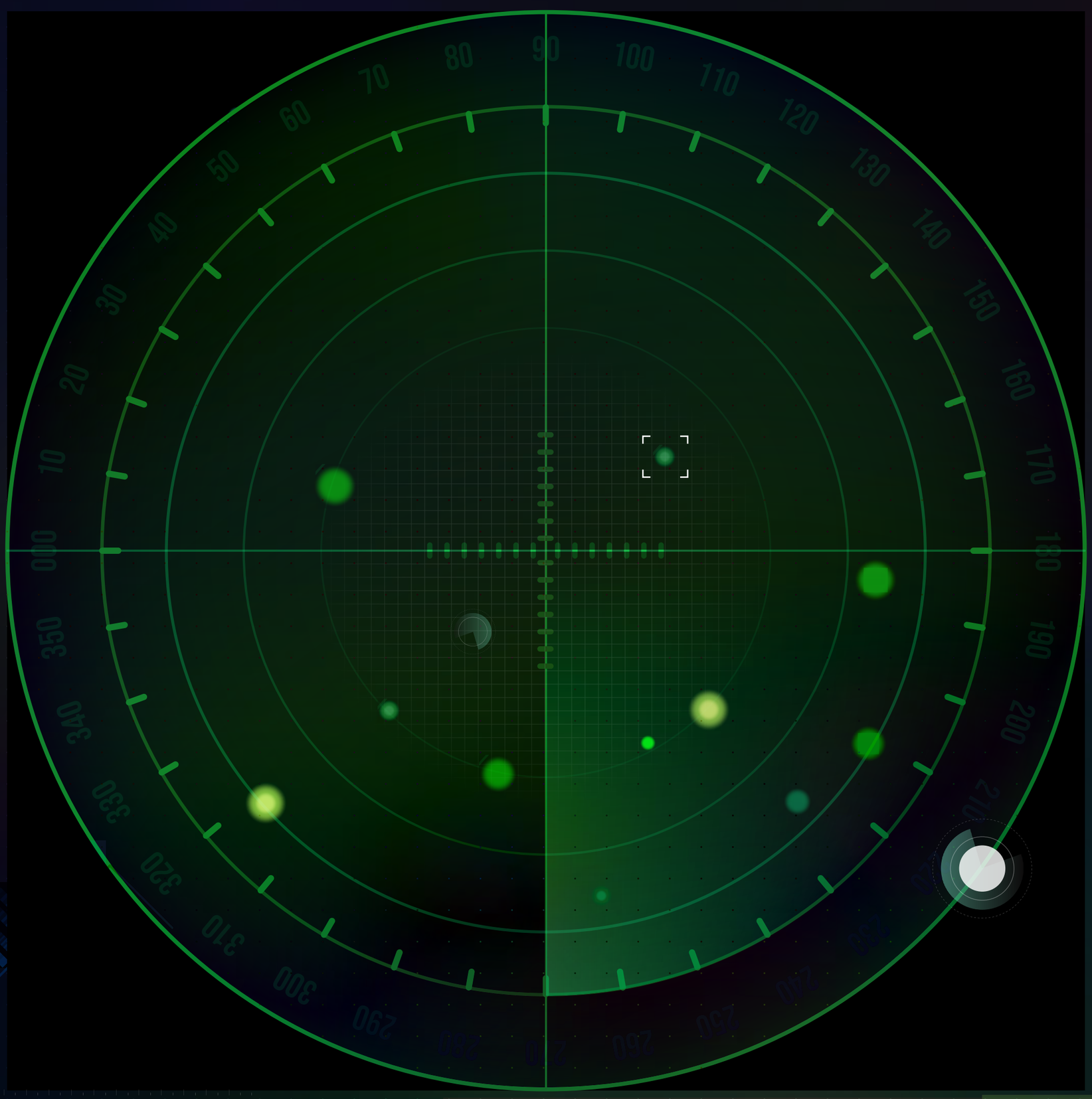
Briskinfosec's

Threatsploit Adversary Report



What you see is never the risk

89th Edition - Jan'2026

Dear Readers,

The speed of modern exploits has created a world where a few hours of hesitation can change the trajectory of an entire company. We are seeing the traditional gap between a bug discovery and a weaponized attack disappear almost entirely. This report is your tactical vantage point, designed to help you see around the corner and understand the specific threats currently reshaping your digital footprint.

The focus has shifted heavily toward the "plumbing" of the enterprise. The exploitation of the n8n RCE and React2Shell vulnerabilities showed that attackers are no longer just knocking on the front door, they are targeting the automation engines and web frameworks that keep your business moving. When these foundational layers are hit, traditional perimeter defenses often fail to trigger, giving adversaries deep access to your core workflows.

At the same time, the arrival of Adversarial AI and sophisticated supply chain attacks has changed the economics of deception. The Glassworm malware wave, which infiltrated developer tools, proves that the environments used to build our digital world are now a primary front. Meanwhile, AI-driven phishing kits are making real-time MFA bypass a standard capability, allowing even mid-tier actors to perform surgical strikes on high-value identities.

These events signal a shift from simple data theft to seeking persistent residency within your cloud. By harvesting tokens from sources like Docker Hub, adversaries build long-term access points that remain silent until the moment of impact. Your advantage isn't found in more tools, but in better timing. This report provides the context to align your strategy with the actual reality of the threat landscape, ensuring your defense remains proactive and decisive.

Best regards,

Briskinfosec Threat Intelligence Team.

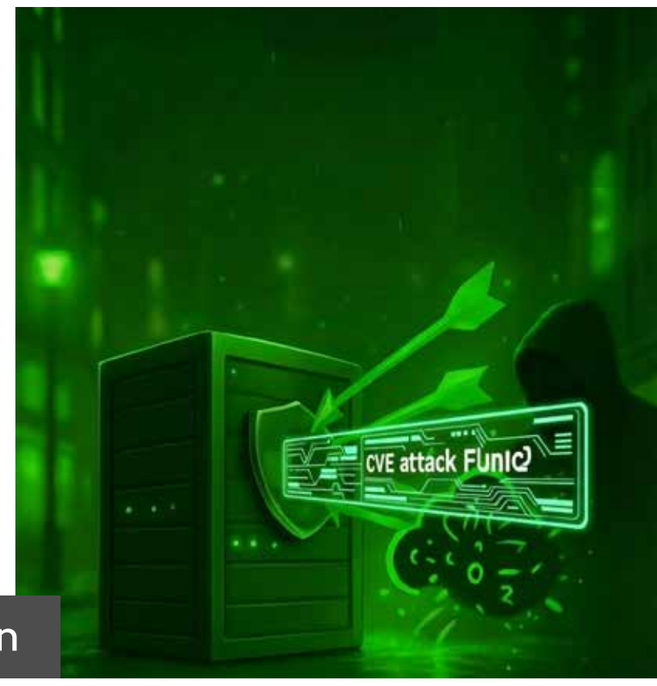
Highlights

1. Critical Infrastructure & Enterprise Vulnerabilities
2. Web & Application Security
3. Ransomware & Evasion Tactics
4. AI & Next-Gen Phishing
5. Advanced Persistent Threats (APT) & State Actors

- Measure your Maturity to Master your Security
- Global Vulnerability Impacts of 2025
- 2025 Industry Cyberattack Breakdown

CRITICAL INFRASTRUCTURE & ENTERPRISE VULNERABILITIES

Cisco warns of active exploitation of unpatched zero-day in AsyncOS email appliances



Cisco warned customers that a maximum severity zero-day in Cisco AsyncOS, tracked as CVE-2025-20393, is being actively exploited by China-aligned actors. The vulnerability impacts physical and virtual appliances with the Spam Quarantine feature enabled. Attackers can execute remote commands with unrestricted root privileges to deploy webshells. Successful exploitation allows full control of the device and persistent unauthorized access.

Attack Type : Zero-Day Exploit / RCE

Cause of Issue : Improper Input Validation

Takeaway : Audit Cisco Email Gateways for indicators of compromise immediately

Fortinet, Ivanti & SAP Urgently Patch Critical Authentication and Code Execution Flaws

Major enterprise vendors issued emergency security patches to address critical vulnerabilities. Fortinet patched a SAML authentication bypass (CVE-2025-59718) that acts as a skeleton key for security appliances. Simultaneously, Ivanti and SAP addressed high-severity code injection flaws that could allow unauthenticated attackers to take full control of business platforms. These flaws are high-priority targets for state-sponsored actors.

Attack Type : Authentication Bypass / RCE

Cause of Issue : Cryptographic Signature Failure

Takeaway : Apply security patches immediately to mitigate remote access risks

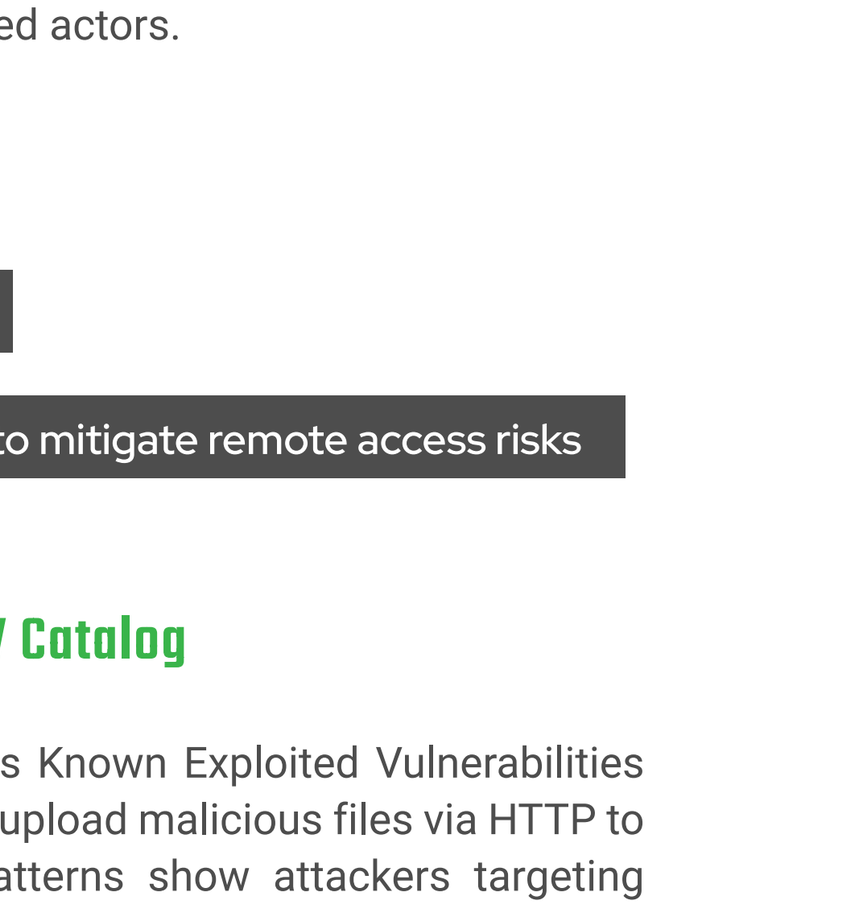
CISA Adds Actively Exploited Sierra Wireless Router RCE Flaw to KEV Catalog

CISA added a critical RCE vulnerability in Sierra Wireless AirLink routers to its Known Exploited Vulnerabilities catalog. Tracked as CVE-2018-4063, the flaw allows authenticated attackers to upload malicious files via HTTP to achieve root privileges. Despite being a legacy bug, recent exploitation patterns show attackers targeting industrial IoT devices to gain initial access to critical infrastructure and corporate networks.

Attack Type : Authentication Bypass / RCE

Cause of Issue : Unrestricted File Upload

Takeaway : Update firmware or replace legacy Sierra Wireless routers as advised



New UEFI flaw exposes motherboards to early-boot DMA attacks

Researchers identified a widespread UEFI firmware vulnerability impacting motherboards from ASRock, ASUS, and MSI. The issue stems from a failure to initialize the IOMMU correctly during the pre-boot phase. This oversight allows physically present attackers to perform Direct Memory Access attacks and inject malicious code before the operating system or security features load. This bypasses nearly all modern software-based security.

Attack Type : Firmware / DMA Attack

Cause of Issue : IOMMU Misconfiguration

Takeaway : Restrict physical access to servers and update BIOS/UEFI firmware

Critical n8n Remote Code Execution (CVE-2025-68613)

A critical vulnerability in the n8n workflow automation platform, tracked as CVE-2025-68613, allows authenticated users to execute arbitrary code. The flaw is caused by improper sanitization of user-controlled inputs within the platform's expression engine. Attackers can leverage expression injection to trigger code execution on the underlying server, potentially leading to a complete system takeover and unauthorized data access.

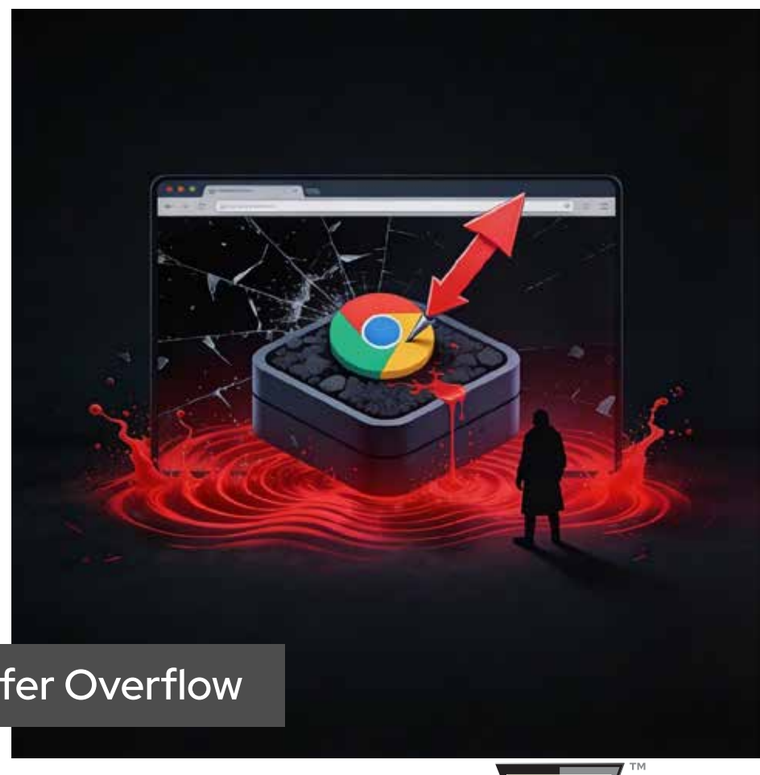
Attack Type : RCE / Expression Injection

Cause of Issue : Improper Input Sanitization

Takeaway : Update n8n to the latest version immediately to prevent takeover

WEB & APPLICATION SECURITY

Chrome Zero-Day Actively Exploited in the Wild



Google released an urgent update for Chrome to patch CVE-2025-14174, a zero-day vulnerability in the ANGLE graphics engine. The flaw is a buffer overflow in the Metal renderer caused by improper buffer sizing. Attackers can exploit this via crafted web content to cause memory corruption, system crashes, or arbitrary code execution. This is the eighth Chrome zero-day exploited in 2025, emphasizing the ongoing risk to browsers.

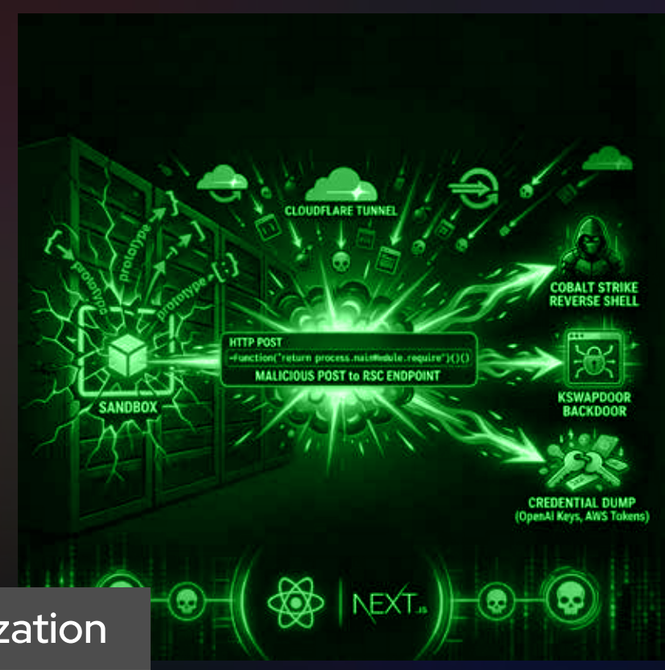
Attack Type : Zero-Day Exploit

Cause of Issue : Memory Corruption / Buffer Overflow

Takeaway : Ensure all browsers are updated to the latest version globally

Critical React2Shell flaw actively exploited in the wild

The React2Shell vulnerability, tracked as CVE-2025-55182, affects React Server Components and frameworks like Next.js. It allows unauthenticated attackers to execute arbitrary code on servers via unsafe deserialization in the React Flight protocol. Exploitation can be achieved with a single malicious HTTP request, leading to prototype pollution. Threat actors have been observed using this flaw to deploy cryptocurrency miners.



Attack Type : Remote Code Execution (RCE)

Cause of Issue : Unsafe Deserialization

Takeaway : Patch React/Next.js dependencies to stop unauthenticated exploits

Apple Security Updates Patch Two WebKit Zero-Days Actively Exploited

Apple issued security updates for iOS, macOS, and Safari to address two WebKit zero-days, including CVE-2025-43529. These use-after-free vulnerabilities allow attackers to execute code by tricking users into processing maliciously crafted web content. Apple confirmed these flaws were used in sophisticated attacks targeting high-profile individuals. The updates improve memory management to prevent these memory corruption exploits.

Attack Type : Zero-Day Exploit

Cause of Issue : Use-After-Free Vulnerability

Takeaway : Update all iOS, macOS, and iPadOS devices to current versions

Glassworm Malware Resurfaces with Third Wave of Malicious VS Code Extensions

The Glassworm supply-chain malware has returned, distributing 24 malicious VS Code extensions. The malware uses invisible Unicode and Private Use Area characters to hide malicious code during reviews, making it nearly impossible to detect visually. It steals developer credentials and cryptocurrency wallet data while leveraging the Solana blockchain for its command and control. This wave marks a significant evolution in supply chain worms.

Attack Type : Supply Chain / Malicious Extensions

Cause of Issue : Unicode Obfuscation

Takeaway : Verify VS Code extensions and limit developer permissions for keys

BriskInfosec
VULNERABILITY TO VICTORY
www.briskinfosec.com

Malicious WhatsApp API npm package steals messages and credentials

Security researchers identified a malicious npm package named lotusbail that impersonates a legitimate WhatsApp API library. Once integrated into a project, the package secretly intercepts private messages, contact lists, and authentication tokens. The stolen data is then exfiltrated to the attacker's server. This supply chain attack demonstrates the persistent threat of poisoned open-source libraries used in modern application development.

Attack Type : Supply Chain / Credential Theft

Cause of Issue : Malicious Package Injection

Takeaway : Audit all npm dependencies and monitor for unauthorized exfiltration

RANSOMWARE & EVASION TACTICS

VolkLocker Ransomware Exposed by Hard-Coded Master Key

A new Ransomware-as-a-Service operation named VolkLocker was recently discovered to have a critical design flaw. Researchers found that the master decryption key was hard-coded directly into the malware binary. This implementation error allows victims to decrypt their files without paying the ransom. Despite this flaw, the ransomware is capable of encrypting both Windows and Linux systems, showing a move toward cross-platform threats.

Attack Type : Ransomware

Cause of Issue : Hard-coded Cryptographic Key

Takeaway : Use the public decryptor if hit; harden systems against RaaS

Ransomware gangs use Shanya EXE packer to hide EDR killers

Ransomware groups like Akira and Medusa are increasingly using the Shanya packer service to evade detection. This service specializes in concealing EDR killers, which are tools designed to disable or terminate endpoint security software. By packing these tools, attackers can execute them undetected, effectively blinding security teams before deploying the final ransomware payload. This tactic significantly increases the success rate of attacks.

Attack Type : Evasion / EDR Disablement

Cause of Issue : Advanced Obfuscation

Takeaway : Deploy behavioral-based EDR that detects security tool tampering

WinRAR CVE-2025-6218 Actively Exploited in the Wild

CISA warned of active exploitation involving a path traversal vulnerability in WinRAR versions prior to 7.12. The flaw, tracked as CVE-2025-6218, allows attackers to place malicious files in sensitive system folders when a victim opens a crafted archive. This can lead to arbitrary code execution or system persistence. The widespread use of WinRAR makes this a high-impact vulnerability that requires immediate patching across organizations.

Attack Type : Path Traversal / RCE

Cause of Issue : Improper Path Handling

Takeaway : Update WinRAR to version 7.12 or higher across all workstations

Phantom Stealer Spread by ISO Phishing Campaign

Operation MoneyMount-ISO is a Russian phishing campaign delivering Phantom Stealer malware. The attack begins with fake payment confirmation emails containing ZIP archives with embedded ISO files. When mounted, the ISO presents an executable disguised as a bank document. Upon execution, the malware harvests credentials, cryptocurrency wallets, and sensitive financial data, exfiltrating it through Telegram bots and Discord webhooks.

Attack Type : Infostealer / Phishing

Cause of Issue : Social Engineering / ISO Mounting

Takeaway : Block ISO file attachments at the email gateway level

MacSync macOS stealer uses signed app to bypass Apple Gatekeeper

A new variant of the MacSync macOS information stealer has been identified using a digitally signed and notarized Swift application to bypass Apple Gatekeeper. Disguised as a messaging app installer, the malware is delivered via a DMG file. Once run, it bypasses XProtect security checks and executes a script to steal local data, credentials, and keys. Apple has since revoked the certificate, but the incident highlights the abuse of trust.

Attack Type : Infostealer / Malware

Cause of Issue : Certificate Abuse

Takeaway : Review and monitor for unknown notarized apps in macOS environments

BriskInfosec™
VULNERABILITY TO VICTORY
www.briskinfosec.com

AI & NEXT-GEN PHISHING

Malicious AI Models Lower Barrier to Advanced Cyberattacks

The emergence of malicious large language models like WormGPT 4 is lowering the barrier for entry into cybercrime. These unrestricted AI models allow low-skill attackers to generate sophisticated ransomware code and highly polished phishing lures. By automating the creation of attack tools, these models scale the volume and complexity of threats, making traditional security filters less effective against highly tailored AI content.

Attack Type : AI-Assisted Cybercrime

Cause of Issue : Malicious LLM Availability

Takeaway : Strengthen phishing detection to counter AI-generated content

New AI-Enabled Phishing Kits Use MFA Bypass to Steal Credentials

Advanced phishing kits such as BlackForce and Spiderman are now incorporating AI to automate credential theft. These kits utilize Man-in-the-Browser techniques to capture real-time multi-factor authentication codes. By displaying fake authentication pages while the attacker logs into the legitimate site, they bypass traditional MFA protections. These kits are often sold as subscription services on Telegram, making them widely accessible.

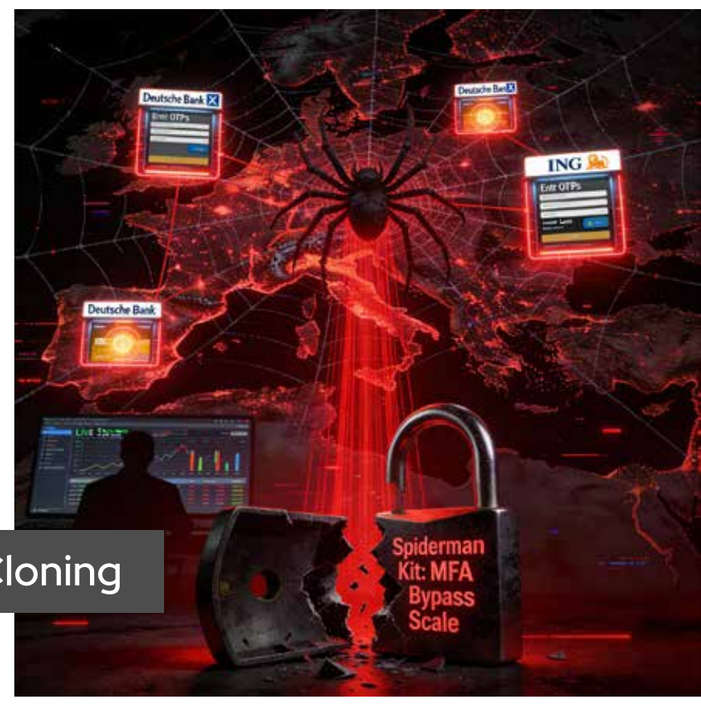
Attack Type : Phishing / MFA Bypass

Cause of Issue : Automated Session Injection

Takeaway : Transition to FIDO2/WebAuthn for phishing-resistant MFA

New Spiderman phishing kit targets European banks and crypto users

The Spiderman phishing kit is specifically targeting customers of major European banks and cryptocurrency services. It creates pixel-perfect replicas of login pages to steal credentials, two-factor authentication codes, and cryptocurrency seed phrases. The kit uses geofencing and device filtering to ensure only targeted users see the malicious pages, evading security scanners and researchers while focusing on high-value financial assets.



Attack Type : Credential Phishing

Cause of Issue : Social Engineering / Site Cloning

Takeaway : Educate users on verifying URL authenticity for banking logins

2025 phishing trends show omni-channel attacks and MFA bypass evolution

Phishing trends for 2025 reveal a shift toward omni-channel attacks, moving beyond email to platforms like LinkedIn and search ads. Threat actors are increasingly using session theft and consent phishing to bypass multi-factor authentication. These attacks often leverage AI-generated images and videos to impersonate brands with high fidelity, making it difficult for even savvy users to distinguish between legitimate and fake communications.

Attack Type : Social Engineering

Cause of Issue : Identity & Session Abuse

Takeaway : Implement identity-centric defenses and session monitoring

Fake OSINT and GPT Utility GitHub Repos Spread PyStoreRAT Malware

Malware campaigns are leveraging GitHub to distribute a JavaScript-based Remote Access Trojan dubbed PyStoreRAT. Attackers host repositories themed as OSINT tools or GPT wrappers to appeal to developers. These repos contain loader stubs that silently download and execute malicious payloads via mshta.exe. The malware profiles systems and steals cryptocurrency files while achieving persistence through scheduled tasks disguised as system updates.

Attack Type : Supply Chain / Trojan

Cause of Issue : Malicious Repository Trust

Takeaway : Verify the reputation and source code of GitHub utilities before use

ADVANCED PERSISTENT THREATS (APT) & STATE ACTORS

China-aligned threat group uses Windows Group Policy to deploy malware

A China-aligned threat actor, LongNosedGoblin, has been identified targeting government networks using Windows Group Policy. By compromising Active Directory, the group distributes custom malware disguised as legitimate policy files. This technique allows them to bypass perimeter defenses and maintain long-term access for espionage. Their primary backdoor, NosyDoor, uses cloud storage like OneDrive for its command and control infrastructure.

Attack Type : APT Espionage

Cause of Issue : Active Directory Abuse

Takeaway : Audit GPO changes regularly for unauthorized lateral movement

Kimsuky spreads DocSwap Android malware via QR phishing

The North Korean threat actor Kimsuky is distributing DocSwap Android malware through QR-code phishing. Attackers impersonate logistics companies and use QR codes to redirect victims to malicious sites. Once installed, the malware gains extensive permissions to record audio, capture photos, and log keystrokes. It also intercepts SMS messages to bypass two-factor authentication, allowing state actors to gain full control over mobile devices.

Attack Type : Mobile RAT / "Quishing"

Cause of Issue : Social Engineering / QR Codes

Takeaway : Warn employees about the risks of scanning unknown QR codes

APT28 hits Ukrainian UKR.net users with long running credential phishing

Russian state-sponsored group APT28 has conducted a sustained credential-harvesting campaign targeting Ukrainian UKR.net webmail users. The group uses PDF documents with shortened links that lead to fake login pages hosted on legitimate platforms. These pages are designed to steal both login credentials and two-factor authentication codes. This campaign supports broader GRU intelligence requirements amid the ongoing conflict in the region.

Attack Type : State-Sponsored Phishing

Cause of Issue : Targeted Social Engineering

Takeaway : Implement hardware keys for high-value government accounts

Iranian Infy APT resurfaces with updated malware campaigns

The Iranian APT group Infy, also known as Prince of Persia, has reappeared after five years of inactivity. The group is using updated versions of its Foudre downloader and Tonnerre implant to target high-value victims in the Middle East, Europe, and Canada. These updated malware strains are used for system profiling and data exfiltration. The resurgence indicates a renewed focus on long-term cyber espionage and strategic intelligence gathering.

Attack Type : Cyber Espionage

Cause of Issue : Custom Malware Deployment

Takeaway : Update IOCs to include the latest Infy malware signatures

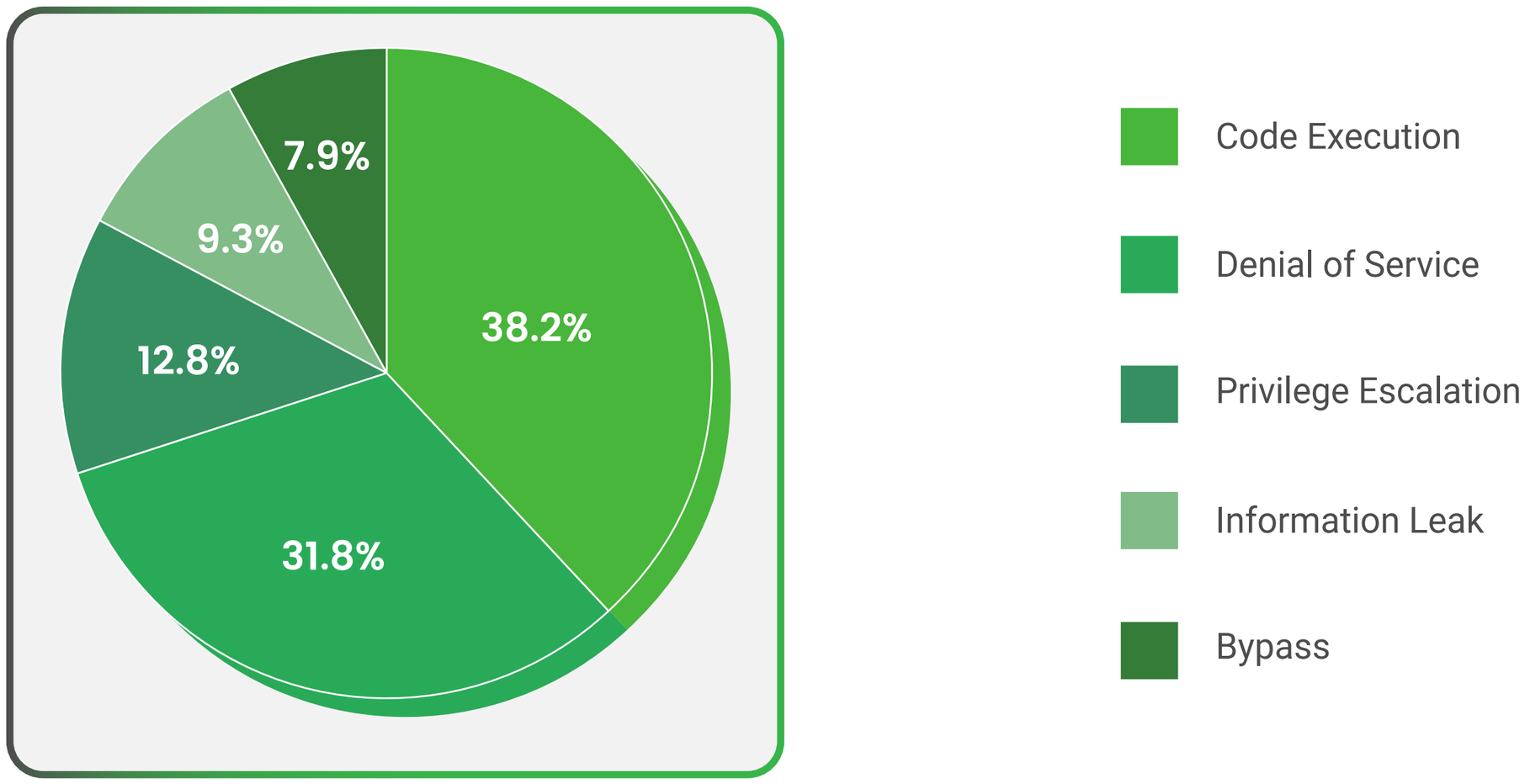
MEASURE YOUR MATURITY TO MASTER YOUR SECURITY

Stop managing vulnerabilities and start measuring resilience. Our bSAFE model evaluates your organization across the 7 critical layers of modern defense to give you a clear, actionable maturity score.

Get Your Score Now

GLOBAL VULNERABILITY IMPACTS OF 2025

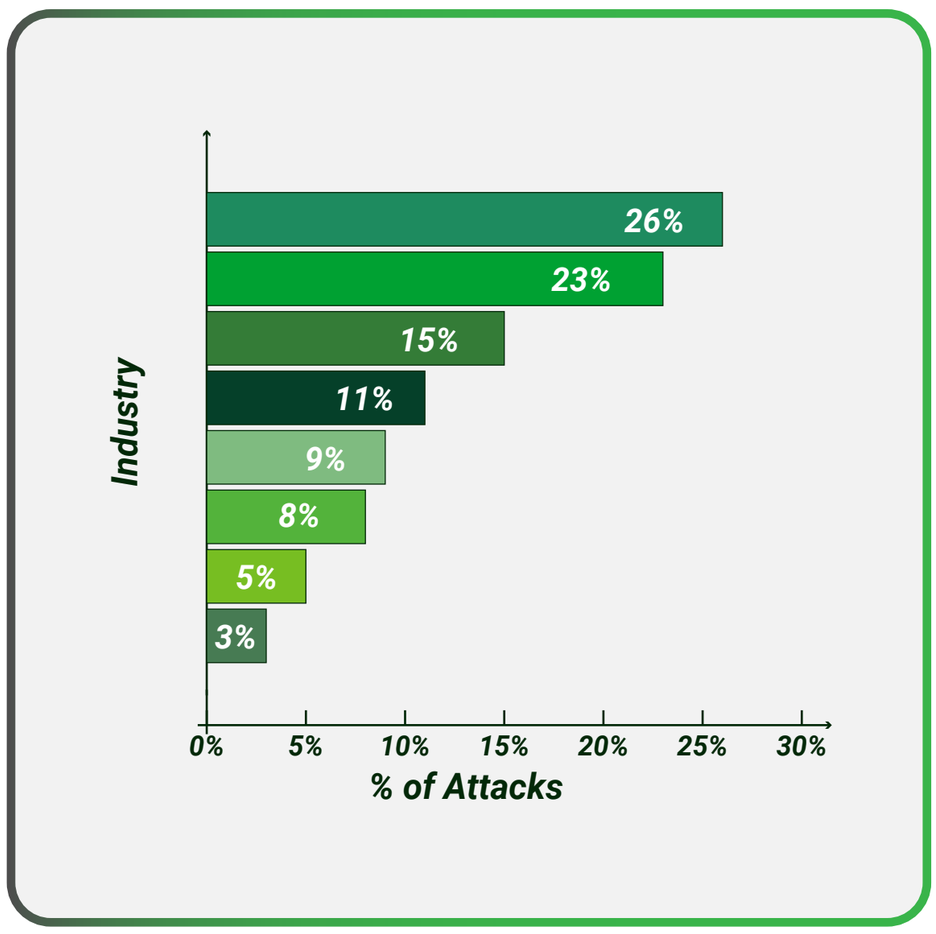
A statistical analysis of the vulnerability outcomes reported this year.



- **Remote Takeover is the Priority :** With Code Execution at #1, attackers are bypassing basic defenses to gain total system control.
- **Continuity is Under Constant Attack :** High DoS numbers show that keeping your business "always-on" requires more than just a firewall.
- **The Danger of Lateral Movement :** Privilege Escalation and Bypass stats prove that once a hacker gets inside, they can quickly become an administrator.
- **Data is the Most Expensive Asset :** Information Leaks remain the highest risk for your brand reputation and regulatory fines.
- **Proactive Detection is Mandatory :** The sheer volume of these impacts shows that waiting for an attack to happen is no longer an option.

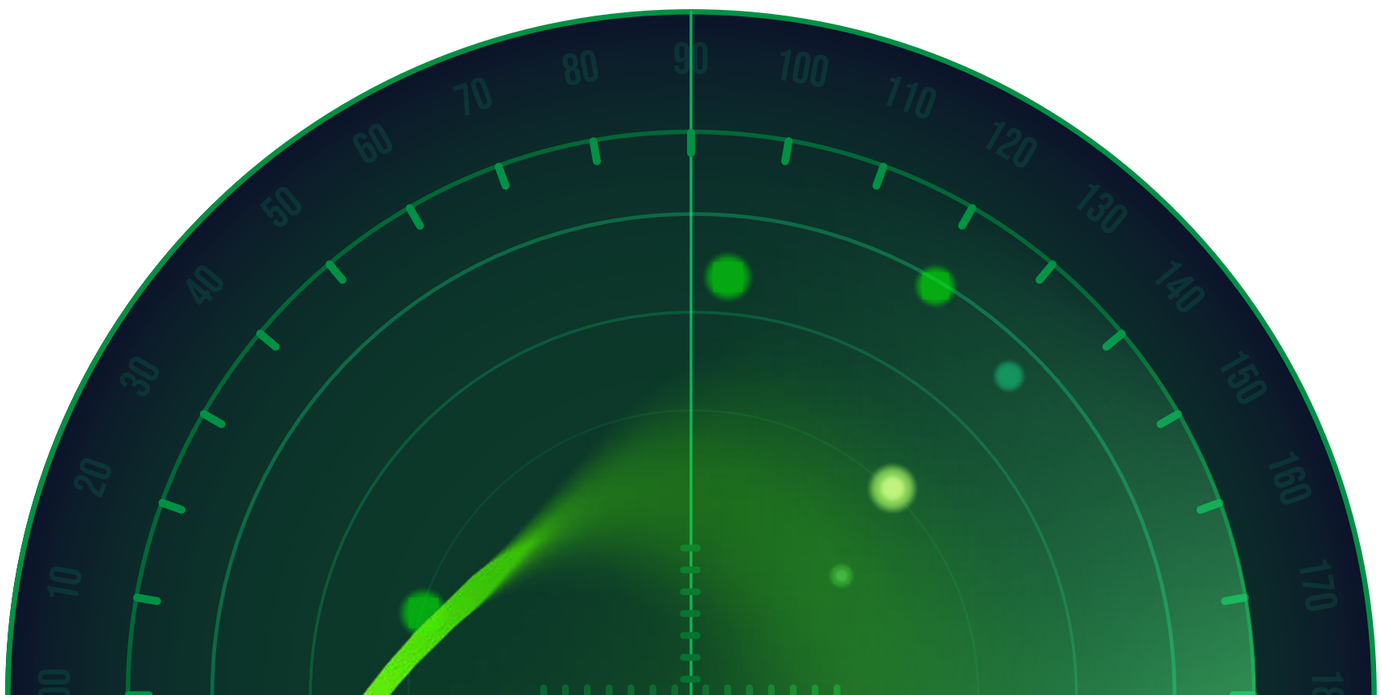
2025 INDUSTRY CYBERATTACK BREAKDOWN

An impact-level analysis of how major sectors were affected by cyber threats this year.



- Manufacturing
- Finance & Insurance
- IT & Technology
- Healthcare
- Education & Research
- Government
- Retail & Wholesale
- Others

- **Operational Resilience in Manufacturing** addresses the high risk of production downtime by enforcing strict segmentation between IT and Operational Technology (OT) to neutralize ransomware extortion.
- **Identity First Security in Finance and Insurance** counters the rise in credential-based access through Zero Trust frameworks and hardware-driven authentication to block unauthorized entry.
- **Supply Chain Accountability in IT and Technology** mitigates cascading breach risks by utilizing Software Bill of Materials (SBOM) and continuous third-party risk evaluations to secure the ecosystem.
- **Data Custodianship in Healthcare** protects against record theft and pure extortion by isolating medical device networks and ensuring the availability of immutable, offline backups.
- **Asset Hardening in Education and Research** secures expansive, open environments by automating legacy system patching and deploying localized phishing simulations to reduce human-centered entry points.
- **Strategic Monitoring in Government** defends against geopolitical espionage and attacks on infrastructure through 24/7 continuous oversight and integration with national threat intelligence.



BriskInfosec™
VULNERABILITY TO VICTORY

www.briskinfosec.com

TRUE RESILIENCE IS
THE ABILITY TO SEE
THE THREAT BEFORE
IT BECOMES A HEADLINE

BriskInfosec™
VULNERABILITY TO VICTORY

www.briskinfosec.com