93rd Edition

May 2026

THREATSPLOIT

Adversary Report

BriskInfosec™
VULNERABILITY TO VICTORY
www.briskinfosec.com

Dear Reader,

Every week, attackers find new ways into systems that organizations believe are secure. This report cuts through the noise and shows exactly what is happening right now, who is attacking, how they are getting in, and what you can do to stop them before it is too late.

Criminals are hiding malicious code inside everyday web traffic, wiping entire systems beyond recovery, and sitting silently inside corporate networks for months without being noticed. One threat group alone has already infected over 1,500 companies. Another is using your own cloud email inbox to send attack commands, making it nearly impossible to tell the difference between normal activity and a breach.

Familiar tools your teams use daily such as VPNs, PDF readers, web browsers, and developer plugins are being turned into entry points. Attackers are also going after AI tools now, slipping harmful code into models that developers download and trust, and tricking AI assistants into leaking private company data without anyone realizing it has happened.

Each threat in this report comes with a clear explanation of what went wrong and one direct action your team can take immediately. No complicated language. No guesswork. Just a straight line between the threat and your next move.

- Briskinfosec Threat Intelligence Team

Section 1 : Malware & Advanced Threats

1. Stealthy Cookie-Controlled PHP Web Shells

Microsoft has revealed a stealthy attack technique where threat actors deploy PHP web shells controlled via HTTP cookies on Linux servers. Instead of using typical request parameters, attackers trigger malicious execution only when specific cookie values are supplied, allowing the payload to remain hidden during normal traffic. Persistence is achieved using cron jobs that recreate the web shell if removed. This method reduces detection visibility and enables long-term unauthorized access to compromised hosting environments.

Attack Type : Webshell

Cause of Issue : Weak Access Control

Takeaway : Implement file integrity monitoring and monitor HTTP cookies for anomalous script execution.

Attack Type : Wiper Malware

Cause of Issue : Targeted Intrusion

Takeaway : Maintain offline backups and strong endpoint protection to prevent destructive payloads.

2. Lotus Wiper Hits Venezuela Critical Sectors

Researchers identified a destructive malware campaign called Lotus Wiper targeting organizations in Venezuela. The malware is designed to overwrite and erase files, leading to irreversible data loss and system disruption. It spreads through targeted intrusion methods and executes wiping routines that impact critical systems and operational continuity. The campaign highlights the use of wiper malware as a strategic tool to disrupt organizations rather than financially monetize attacks by holding the data for ransom.

3. Pre-Stuxnet Fast16 Malware for Sabotage

Researchers uncovered Fast16, a previously undocumented sabotage malware dating back to 2005, predating Stuxnet. The malware targets high-precision engineering and simulation software, silently altering computational results to cause incorrect outputs, system degradation, or physical failures. It includes self-propagation capabilities and operates stealthily within networks. Evidence suggests it may have been used in cyber operations targeting sensitive programs such as nuclear research and strategic infrastructure.

Attack Type : Cyber Sabotage

Cause of Issue : Software Tampering

Takeaway : Strengthen identity management and enable continuous monitoring for lateral movement.

Attack Type : Botnet / Proxy Malware

Cause of Issue : Proxy Malware

Takeaway : Monitor unusual SOCKS5 traffic and audit egress to unauthorized C2 servers.

4. SystemBC Botnet Exposes Corporate Victims

Researchers uncovered a SystemBC command and control server linked to The Gentlemen ransomware group, revealing a botnet with over 1,570 infected systems. The malware acts as a proxy tool, creating encrypted SOCKS5 tunnels that allow attackers to maintain persistence, execute commands, and deploy additional payloads. The majority of infections are tied to corporate environments, indicating targeted intrusion activity. SystemBC plays a key role in ransomware deployment chains by enabling lateral movement.

5. Harvester APT Spreads GoGra via Cloud

The Harvester threat group has deployed a Linux variant of its GoGra backdoor targeting organizations in South Asia. The malware abuses the Microsoft Graph API and Outlook mailboxes as covert command and control channels, blending malicious traffic with legitimate cloud activity to evade detection. Delivered via ELF binaries disguised as PDF files, the backdoor enables remote command execution, data exfiltration, and persistent access. This marks an evolution of Harvester's cross platform espionage capabilities.

Attack Type : APT Espionage

Cause of Issue : Cloud Abuse

Takeaway : Audit cloud API permissions and monitor unusual activity in service accounts.

Attack Type : Ransomware

Cause of Issue : Credential Theft

Takeaway : Implement Zero Trust and layered encryption monitoring to detect rapid file changes.

6. New Variant of Medusa Ransomware

A sophisticated new variant of Medusa ransomware has surfaced, utilizing multiple encryption methods to evade detection. It targets large-scale enterprise data and employs double extortion by threatening to leak sensitive files on a public leak site. The variant shows improved obfuscation to bypass standard antivirus signatures. Attackers are focusing on higher-value targets where downtime has a massive financial impact. This evolution shows that the group is refining its tactics for persistent network access.

7. Infostealer Campaign Exploiting Fake Updates

Attackers are distributing infostealers like Lumma and RedLine through fake browser and software update prompts. These campaigns use SEO poisoning and malvertising to lure users to malicious sites. Once executed, the malware harvests browser credentials, crypto wallets, and session cookies for further exploitation. The scale of these operations indicates a highly organized approach to credential harvesting that facilitates subsequent ransomware attacks. Technical users remain a key target for these stealthy tools.

Attack Type : Infostealer / Phishing

Cause of Issue : Social Engineering

Takeaway : Enforce centralized software management and block unauthorized scripts on workstations.

8. Linux Ransomware Targets Cloud Workloads

A surge in Linux-specific ransomware has been detected targeting cloud-native workloads and ESXi servers. These variants are optimized for speed, encrypting virtual machine disks rapidly to cripple cloud infrastructure. The trend reflects a strategic shift by threat actors toward high-value, high-availability cloud targets where traditional endpoint security often fails. By hitting the hypervisor layer, attackers can impact multiple server instances simultaneously, maximizing their leverage during negotiations.

Attack Type : Cloud Ransomware

Cause of Issue : Cloud Access Risk

Takeaway : Secure cloud admin interfaces with MFA and patch hypervisors against escapes.

Section 2 : Zero-Day Intelligence

9. Windows Kernel Zero-Day (CVE-2026-21412)

A critical zero-day vulnerability in the Windows Kernel allows for local privilege escalation. Attackers can exploit this to gain SYSTEM-level privileges, bypassing security boundaries like BitLocker and Virtualization-Based Security. It is currently being used in targeted attacks against financial institutions. The vulnerability stems from improper handle validation, allowing code execution at the highest level of the operating system. Organizations must prioritize this update to prevent lateral system takeover.

Attack Type : Privilege Escalation

Cause of Issue : Handle Validation

Takeaway : Apply Windows security patches fast and monitor unauthorized privilege changes.

The Dual Frontier

AI for Security and Security for AI

As Artificial Intelligence matures into a core part of how businesses operate, it has created a complex challenge for cybersecurity. Organizations must now master two disciplines at once: using AI to strengthen their defenses and protect their AI systems from being attacked.

AI for Security - The Intelligent Shield

AI gives security teams the ability to do what is humanly impossible at scale, processing massive volumes of data in real time to catch threats before they cause damage.

Behavioral Threat Detection : Identifying unusual patterns in how users access systems, flagging compromised accounts or insider threats that traditional tools would miss.

Automated Incident Response : Security workflows powered by AI that can instantly isolate an infected device or cut off unauthorized access the moment a threat is confirmed.

Predictive Vulnerability Management : Using machine learning to determine which vulnerabilities are most likely to be exploited in your specific environment, enabling smarter and faster patching decisions.

Phishing Defense : AI that reads the language and context of emails to catch sophisticated phishing attempts that slip past conventional filters.

Security for AI - Protecting the Brain

If AI is the shield, it is also a target. Attackers are developing techniques specifically designed to manipulate AI systems from the inside out.

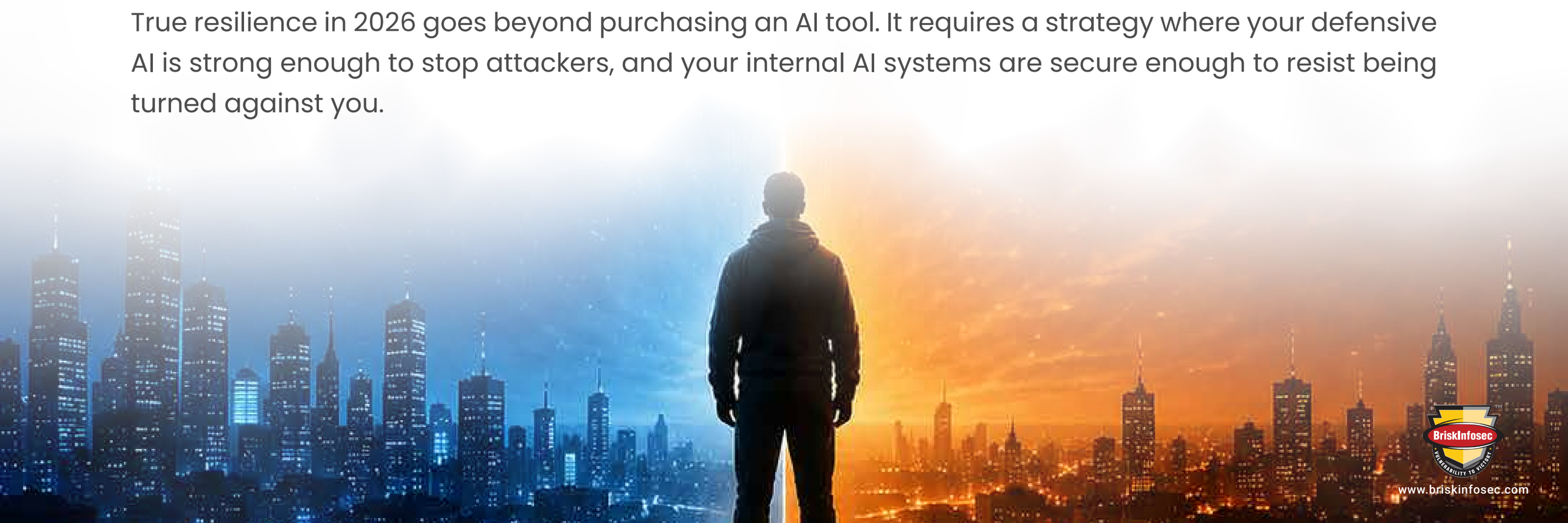
Input Manipulation Defense : Preventing attackers from feeding subtly altered data into AI models to force incorrect decisions or bypass detection entirely.

Training Data Integrity : Ensuring the data used to build AI models has not been tampered with to create hidden weaknesses that attackers can trigger later.

Model Protection : Stopping competitors or attackers from reverse engineering proprietary AI systems by studying how they respond to repeated queries.

Prompt Firewalling : Protecting AI assistants from being manipulated through crafted instructions that trick them into bypassing safety controls or exposing sensitive information.

True resilience in 2026 goes beyond purchasing an AI tool. It requires a strategy where your defensive AI is strong enough to stop attackers, and your internal AI systems are secure enough to resist being turned against you.



BriskInfosec
VULNERABILITY TO VICTORY

www.briskinfosec.com

Attack Type : Remote Code Execution

Cause of Issue : Input Validation

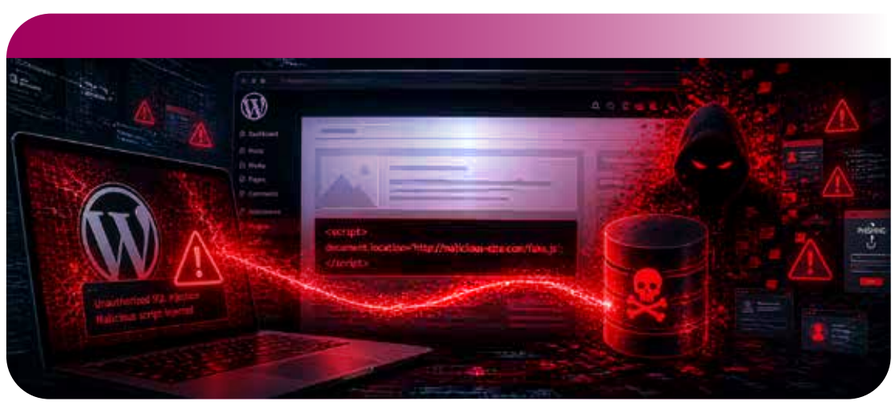
Takeaway : Restrict SD-WAN console access to trusted IPs and prepare for urgent updates.

10. Cisco SD-WAN Zero-Day Exploited in the Wild

Adversaries are actively exploiting an unpatched vulnerability in Cisco SD-WAN software to execute arbitrary code with root privileges. This allows attackers to intercept network traffic and gain full control over wide-area network infrastructure, posing a major risk to global enterprise connectivity. The flaw involves a logic error in the management interface that processes unauthenticated inputs. Security teams should restrict management access to trusted IP ranges until a permanent firmware fix is deployed.

11. WordPress SEO Plugin Zero-Day Exploitation

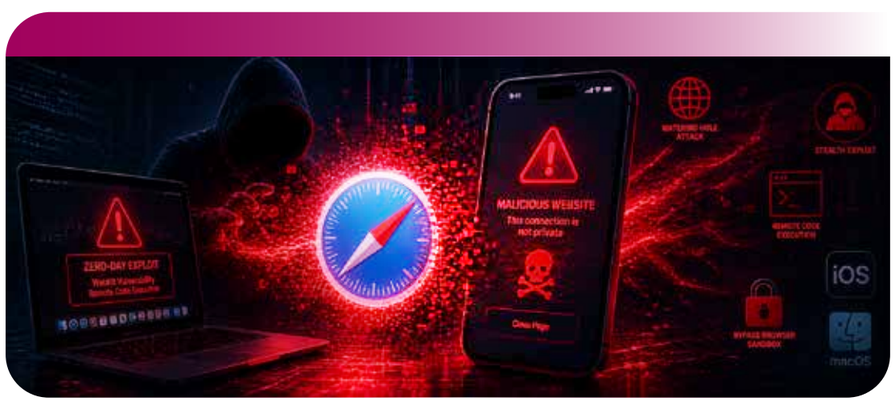
A high-severity zero-day in a widely used SEO plugin for WordPress allows unauthenticated attackers to inject malicious scripts into the site database. This leads to complete site takeover and the redistribution of malware to visiting users. Thousands of sites have already been compromised, with attackers using the access to deploy phishing pages and steal user data. The vulnerability highlights the risk of third-party plugins in public-facing web applications. A web application firewall is highly advised.



Attack Type : SQL Injection

Cause of Issue : Unsafe DB Queries

Takeaway : Disable affected plugin until patched and implement a Web Application Firewall.



Attack Type : Remote Code Execution

Cause of Issue : WebKit Memory Bug

Takeaway : Ensure all iOS and macOS devices are updated to the latest versions to mitigate WebKit risks.

12. Safari Browser Zero-Day (CVE-2026-32890)

A zero-day vulnerability in Apple's WebKit engine allows for remote code execution when a user visits a maliciously crafted webpage. This exploit is being used in watering hole attacks to target specific high-profile individuals by compromising their mobile devices silently. The memory corruption flaw allows an attacker to bypass browser sandboxing to execute arbitrary commands. Users across iOS and macOS platforms are urged to update to the latest versions to mitigate the risk of driveby download infections.

13. Zero-Day in Ivanti Connect Secure VPN

A newly discovered zero-day in Ivanti VPN appliances allows for unauthenticated remote command execution. Attackers are using this to bypass multi-factor authentication and gain initial access to corporate internal networks. This vulnerability is being actively weaponized by state-sponsored actors for long-term espionage and data theft. Because the flaw exists in a core web component, it is difficult to detect without specialized integrity tools. Immediate mitigation is required for all exposed appliances.

Attack Type : Authentication Bypass

Cause of Issue : VPN Web Logic Flaw

Takeaway : Run Ivanti Integrity Checker now and apply latest vendor mitigations.

Attack Type : Arbitrary Code Execution

Cause of Issue : Use-After-Free Bug

Takeaway : Enable Adobe Protected Mode and Enhanced Security until official patches arrive.

14. Adobe Acrobat Zero-Day Exploited via PDFs

Threat actors are distributing specially crafted PDF files that exploit a zero-day in Adobe Acrobat to execute malicious code upon opening. This zero-click or low-click exploit allows for the delivery of backdoors directly to a user's system without further interaction. The vulnerability stems from a use-after-free error in the JavaScript engine used by the application. Until a patch is finalized, organizations should enforce strict viewing policies and use isolated environments for opening attachments.

Section 3 : Vulnerabilities & Exploits

15. Critical Struts RCE (CVE-2026-44321)

A critical vulnerability in Apache Struts allows attackers to execute remote code by sending a manipulated OGNL expression. This vulnerability is similar to the one used in the Equifax breach, making it a high-priority target for automated scanning and mass exploitation across global enterprises. The flaw resides in how the framework handles specific tag attributes, allowing an attacker to run arbitrary system commands. Organizations should prioritize upgrading to the latest patched version of the library.

Attack Type : Remote Code Execution

Cause of Issue : OGNL Expression Bug

Takeaway : Upgrade to the latest Apache Struts version and disable unused OGNL features.

Attack Type : Privilege Escalation

Cause of Issue : Heap Buffer Overflow

Takeaway : Update the sudo package across all Linux servers and workstations immediately.

16. Linux sudo PrivEsc (CVE-2026-3114)

A vulnerability in the sudo utility allows a local user to gain root access by exploiting a heap-based buffer overflow. This flaw affects almost all modern Linux distributions and can be used as a secondary step in an attack to gain full control over a compromised host. The issue occurs when sudo parses specific command-line arguments in an incorrect way, leading to memory corruption. Security teams must ensure that all servers and development environments are updated with the latest security patches.

17. GitLab Auth Bypass (CVE-2026-1150)

GitLab has patched a critical vulnerability that allowed attackers to bypass authentication and gain unauthorized access to private repositories. By manipulating specific session parameters, an attacker could impersonate high-privileged users and steal sensitive source code and proprietary keys. The logic flaw was found in the session management module, affecting both community and enterprise editions. Administrators are urged to update their instances to the latest version to prevent unauthorized exposure.

Attack Type : Authentication Bypass

Cause of Issue : Session Validation Bug

Takeaway : Update GitLab instances to version 17.x or later and audit user access logs for suspicious logins.

Attack Type : Privilege Escalation

Cause of Issue : Path Validation Flaw

Takeaway : Update FortiClient and restrict admin permissions on endpoint devices.

18. FortiClient Vulnerability (CVE-2026-2580)

A high-severity vulnerability in FortiClient allows for local privilege escalation. An attacker with limited access to a workstation can exploit this flaw to gain administrative privileges, potentially disabling local security controls or exfiltrating sensitive data. The issue stems from improper path validation when the application handles internal file operations. This can be used as a pivot point for deeper network penetration. Security managers should verify that all endpoints are running the latest version.

Monthly Intelligence Spotlight

Phishing Simulation Reveals How Employees Respond to a Fake CEO Email

A phishing simulation using a fake CEO email exposed how employees react under pressure. Many trusted authority cues, clicked quickly, and risked compromise, highlighting the urgent need for awareness training.

Read More

The Hidden Risk of Data Leakage in AI Code Assistants

AI code assistants boost productivity but risk leaking sensitive data via prompts, repo access, and cloud processing. Without governance, secrets can be exposed silently.

Read More

Your Former Employees Still Have Access to Your Systems and Data

Former employees often retain access due to poor offboarding, exposing emails, data, and systems. These forgotten accounts can lead to breaches, leaks, or misuse if not promptly removed.

Read More

19. Redis RCE Vulnerability (CVE-2026-2009)

A vulnerability in Redis allows for remote code execution when specific commands are executed with malicious input. This is particularly dangerous for Redis instances exposed to the internet or accessible via insecure internal networks. The flaw occurs within the Lua scripting engine, where an attacker can trigger memory corruption. Organizations should ensure that all Redis instances are password-protected and that access is restricted to trusted IPs only through firewalls and VPC security group settings.

Attack Type : Remote Code Execution

Cause of Issue : Input Validation Error

Takeaway : Password-protect all Redis instances and restrict access to trusted IP ranges.

20. Confluence Vulnerability (CVE-2026-2621)

A vulnerability in Confluence Data Center and Server allows unauthenticated attackers to execute arbitrary code. This exploit is being actively used by ransomware groups to compromise corporate documentation servers and steal internal data. The flaw is linked to improper parameter handling in the web application layer, allowing for the injection of malicious commands. Given its critical nature, all on-premise Confluence instances should be patched immediately or taken offline until the update is applied.

Attack Type : Remote Code Execution

Cause of Issue : Parameter Handling

Takeaway : Patch Confluence immediately and block direct internet access to instances.

21. ESXi Hypervisor Escape (CVE-2026-2888)

A vulnerability in VMware ESXi allows an attacker with local administrative privileges on a virtual machine to execute code on the host hypervisor. This virtual machine escape is a high-impact flaw that can compromise the entire cloud infrastructure. The memory corruption issue occurs in the virtual USB controller component. Organizations should prioritize patching their hypervisor hosts and disabling any unnecessary virtual hardware to reduce the attack surface available to potential malicious actors.

Attack Type : Hypervisor Escape

Cause of Issue : Memory Corruption

Takeaway : Apply latest ESXi patches and disable unnecessary virtual hardware components.

Attack Type : Remote Code Execution

Cause of Issue : Race Signal Condition

Takeaway : Update OpenSSH immediately and restrict SSH access to known, trusted networks only.

22. Vulnerability in OpenSSH (CVE-2026-3000)

A race condition vulnerability in OpenSSH's sshd allows unauthenticated remote code execution with root privileges. This flaw, dubbed RegreSSHion 2, targets the foundational security of remote Linux management and is highly critical for internet-facing servers. An attacker can exploit this during the authentication phase to gain full control of the machine. The fix requires an immediate update of the OpenSSH package. Administrators should also consider limiting SSH access to known and trusted networks only.

Section 4 : DevSecOps & AI Governance

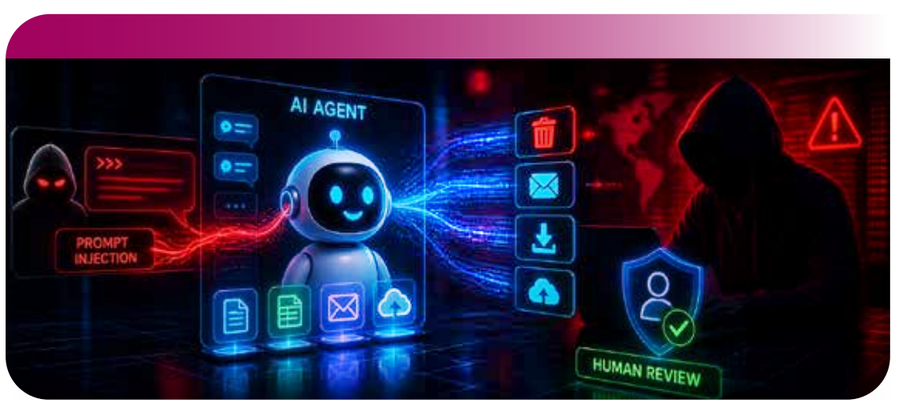
23. Malicious AI Models on Hugging Face

Security researchers have identified multiple malicious AI models on Hugging Face that contain embedded backdoors. When a developer downloads and runs these models, they execute hidden code that exfiltrates API keys and environment variables to an external server. This type of attack targets the fast-growing AI development sector by hiding malware in popular open-source assets. Developers should only use verified models and perform automated security scans on model weights before integration into workflows.

Attack Type : Model Poisoning

Cause of Issue : Auto Scan Not Found

Takeaway : Only use verified AI models and scan all downloaded weights for malicious code.



Attack Type : Prompt Injection

Cause of Issue : LLM Input Sanitization

Takeaway : Implement strict output validation and human-in-the-loop checks for AI-driven actions.

24. AI Agent Prompt Injection in Workflows

Adversaries are using prompt injection techniques to manipulate enterprise AI agents into performing unauthorized actions, such as deleting files or sending sensitive data to external emails. These attacks exploit the direct integration of AI agents into corporate productivity suites. By feeding the agent malicious input, attackers can bypass safety filters and gain access to private internal data. Security teams must implement strict output validation and human-in-the-loop checks for all AI-driven actions.

25. Secret Leakage in GitHub Action Logs

A surge in unintentional secret leakage has been detected within public GitHub Action logs. Developers are accidentally printing API keys and database credentials to the console during build processes, which are then harvested by automated bots. This exposure can lead to full compromise of cloud environments and data platforms. Organizations should enforce the use of secret management tools and enable automated scanning features in their CI/CD pipelines to block the deployment of any exposed credentials.

Attack Type : Information Disclosure

Cause of Issue : CD Secrets

Takeaway : Use specialized secret management tools and enable GitHub's secret scanning feature.

26. Malicious GitHub Copilot Extensions

Attackers have published malicious extensions for GitHub Copilot that appear to provide extra features but actually harvest source code and transmit it to an external server. This highlights a new frontier in targeting the tools that developers rely on for daily coding. The extensions use social engineering to trick developers into granting high-level permissions. Organizations must establish a centralized policy for allowed IDE extensions and monitor for unauthorized network activity from dev systems.

Attack Type : Supply Chain

Cause of Issue : Extension Verify Fail

Takeaway : Establish a centralized policy for IDE extensions and monitor for unauthorized network activity.

27. Insecure Docker Desktop Configurations

Many developers are running Docker Desktop with insecure configurations that allow containers to escape to the host system. Attackers are exploiting these misconfigured environments to gain control over developer workstations and move laterally into corporate networks. The issue often involves running containers with root privileges or mounting sensitive host directories. Enforcing hardened Docker policies and using non-root containers for all development tasks is critical to securing the local workstation.

Attack Type : Container Escape

Cause of Issue : Docker Default Risk

Takeaway : Enforce hardened Docker policies and use non-root containers for development tasks.

Attack Type : Data Leakage

Cause of Issue : Unapproved AI Tools

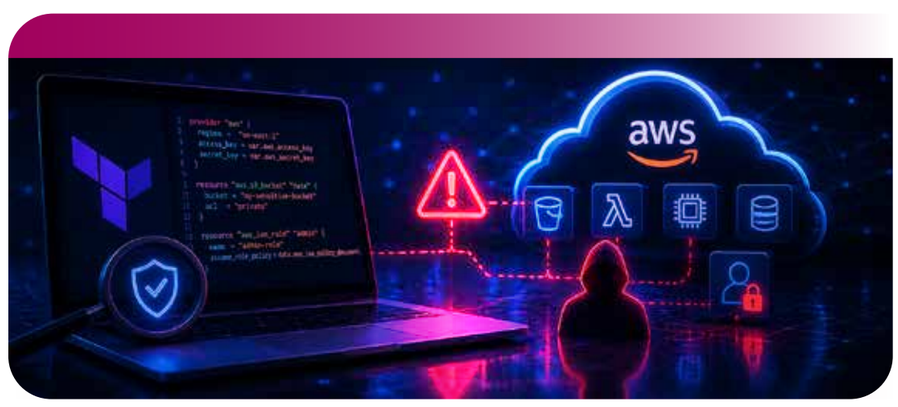
Takeaway : Provide secure enterprise AI platform and enforce DLP for public LLM usage.

28. Shadow AI: Data Leakage in the Enterprise

Organizations are seeing a massive increase in Shadow AI, where employees use unauthorized LLMs to process sensitive corporate data. This results in the loss of intellectual property as data is often used to train public models, bypassing all corporate security controls. The lack of visibility into these tools creates a significant compliance risk for regulated industries. Providing employees with a secure, enterprise-grade AI platform and implementing DLP controls for public sites is a necessary defense.

29. Vulnerability in Terraform Provider for AWS

A vulnerability in a widely used Terraform provider for AWS could allow an attacker to gain unauthorized access to cloud resources. By manipulating specific configuration parameters, an attacker could escalate their privileges within the target AWS environment. The flaw demonstrates the risk of Infrastructure-as-Code where a single insecure default can lead to wide-scale exposure. It is vital to update all Terraform providers to the latest versions and implement automated security scanning for all files.



Attack Type : Privilege Escalation

Cause of Issue : IaC Validation Flaw

Takeaway : Update all Terraform providers to latest versions and use automated IaC security scanning.

Attack Type : Data Poisoning

Cause of Issue : Data Integrity Risk

Takeaway : Use diverse verified data sources for AI training and perform regular bias/trigger testing.

30. Data Poisoning of AI Training Sets

Attackers are poisoning public datasets used for training AI models to introduce specific biases or triggers that they can exploit later. This form of adversarial machine learning can lead to models that make incorrect or malicious decisions in production environments. The stealthy nature of data poisoning makes it difficult to detect after the model has been trained. Using diverse and verified data sources for training and performing regular bias and trigger testing on models is essential for safety.

Nine Years of Resilience

Defining the Future of Cybersecurity

We recently gathered to commemorate a defining milestone established by the 9th Anniversary of our journey. For nearly a decade, we have stood as a dedicated shield for our partners, evolving from a vision of robust defense into a leading force in the cybersecurity landscape.

To celebrate this achievement, our team moved from the operations center to the arena for a day of high energy engagement and camaraderie.

Innovation in Motion :

"The Cyber-Reel competition showcased our team's skill in simplifying security stories creatively."

The Spirit of Challenge:

"Strategy contests tested our teamwork and problem-solving, proving our strength is collective intelligence."

Honoring Our Pillars:

"The highlight was awarding special prizes to those showing exceptional dedication and technical skill."

As we celebrate these nine years of growth, our mission remains unchanged to outpace the adversary and secure the digital future with technical precision and unwavering integrity.

Clear vision is the only defense
against threats right in front of you...!

BriskInfosec™

VULNERABILITY TO VICTORY

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