THREATSPLOIT

ADVERSARY REPORT

94TH EDITION, JUNE 2026

BriskInfosec
VULNERABILITY TO VICTORY

www.briskinfosec.com

Dear Reader,

Attackers continuously uncover new vulnerabilities in systems deemed secure, constantly evolving their tactics to compromise the integrity of global digital infrastructure. Staying ahead requires a clear understanding of who is attacking, the methods they are using, and the precise technical actions required to secure your organization.

We are observing a surge in infrastructure-aware campaigns targeting the developer ecosystem at scale. From self-propagating supply chain worms and compromised maintainer accounts to automated commit injections, the integrity of our software pipelines is increasingly at risk. Adversaries are prioritizing the theft of credentials and session tokens to establish persistent, long-term access, frequently camouflaging their actions as routine administrative tasks.

Simultaneously, enterprise management platforms and network edge appliances remain primary targets. With zero-day exploits targeting critical infrastructure and a rise in sophisticated false-flag operations, the line between legitimate administrative traffic and malicious intrusion has become dangerously blurred.

Each entry in this report provides a clear analysis of the root cause and a direct, actionable recommendation. There is no guesswork or unnecessary complexity, just a strategic path to strengthening your defenses against the latest adversary techniques.

Briskinfosec Threat Intelligence Team

Supply Chain & Developer Ecosystems

1. Mini Shai-Hulud Compromises AI npm

The TanStack npm supply chain compromise, assigned CVE-2026-45321 with a CVSS score of 9.6, impacted 42 packages and 84 versions and propagated via a self-replicating worm dubbed Mini Shai-Hulud. The campaign, attributed to TeamPCP, also affected Mistral AI, Guardrails AI and OpenAI-related ecosystems. Detection began on May 11, 2026, and stolen GitHub workflow tokens enabled lateral movement into downstream repositories.

Attack Type : Self-propagating supply chain worm

Cause of Issue : Maintainer account compromise

Takeaway : Self-propagating supply chain attacks demonstrate the massive risk of relying on automated trust within CI/CD pipelines.

2. Grafana GitHub Breach via TanStack npm

Grafana confirmed a GitHub breach originating from the TanStack npm supply chain attack orchestrated by TeamPCP. Detected on May 11, 2026, the incident exposed source code repositories after a missed workflow token allowed attackers to access GitHub repos despite Grafana's initial rotation. The company received an extortion demand on May 16, 2026 but refused to pay. A data extortion crew named CoinbaseCartel listed Grafana on its dark web leak site on May 15, 2026.

Attack Type : Source code theft and extortion

Cause of Issue : Workflow token rotation gap

Takeaway : Even after rotating credentials, attackers can maintain persistence if secondary tokens or access points are overlooked.

3. Popular node-ipc Package Compromised

Hackers injected credential-stealing malware into a widely downloaded npm package to harvest identities and gain control over modern software delivery infrastructure. The malicious code was designed to be subtle, allowing it to remain undetected while collecting SSH keys and cloud environment variables. By compromising such a popular package, the attackers leveraged the reach of the software supply chain to target a massive number of developer environments, significantly increasing the probability of a high-value breach.

Attack Type : Supply chain credential theft

Cause of Issue : Maintainer compromise

Takeaway : Supply chain attacks now focus on credential harvesting for persistent, infrastructure-level access.

4. Mini Shai-Hulud Pushes Malicious npm

In May 2026, Datadog and other researchers identified a fresh wave of the Mini Shai-Hulud campaign that compromised packages in the @antv ecosystem, including echarts-for-react. With combined weekly downloads exceeding 1.1 million, the affected packages exposed downstream developers to credential theft. The attack escalated after TeamPCP open-sourced the original Shai-Hulud framework as part of a supply chain attack contest announced on BreachForums.

Attack Type : Supply chain credential theft

Cause of Issue : Maintainer account compromise

Takeaway : Open-sourcing attack frameworks on forums accelerates the pace at which supply chain threats propagate.

5. Malicious npm Packages Deliver DDoS

Researchers identified four malicious npm packages, including a clone of the Shai-Hulud source code, designed to siphon SSH keys and cloud credentials or deploy a Golang-based DDoS botnet. These packages, appearing as legitimate utilities, targeted developer machines to harvest credentials. The incident demonstrates the persistent threat posed by typosquatting and how open-source repositories can be weaponized to distribute malware to developers and build systems.

Attack Type : Supply chain infostealer and DDoS

Cause of Issue : Typosquatting & Shai-Hulud Clones

Takeaway : Public package registries remain a battleground for deploying credential-stealing malware into dev environments.

6. Megalodon Attack Pushes Malicious Code

The Megalodon campaign automated malicious commit injections across 5,561 GitHub repositories using stolen session tokens derived from infostealer-infected systems. The scale of the automation, combined with legitimate developer credentials, allowed threat actors to push malicious code into numerous downstream projects. This incident illustrates the automated efficiency attackers use to exploit the developer ecosystem at scale, leveraging trust in commit history.

Attack Type : Supply Chain Commit Injection

Cause of Issue : Infostealer-stolen GitHub tokens

Takeaway : Automated campaigns can scale attacks against thousands of targets using compromised developer credentials.

Critical Infrastructure & Network Edge

7. SonicWall Gen6 SSL-VPN Brute-Forced

Threat actors targeted legacy SonicWall SSL-VPN appliances by brute-forcing credentials and bypassing multi-factor authentication to deploy ransomware post-exploitation. The campaign specifically prioritized older devices that were likely not fully hardened or lacked modern authentication protections. By exploiting these critical network gateways, the actors gained immediate access to the internal network. This highlights the ongoing risk posed by legacy edge infrastructure that is not maintained or secured with robust MFA controls.

Attack Type : Credential brute force

Cause of Issue : Weak credentials and MFA bypass

Takeaway : Legacy network edge appliances remain the most common initial access point for ransomware actors if not patched and secured.

8. Ubiquiti Patches UniFi OS Issues

In May 2026, Ubiquiti released security updates for three maximum-severity vulnerabilities in UniFi OS that allow remote attackers without privileges to compromise affected systems. The flaws can be exploited without authentication and pose significant risk to large fleets of UniFi devices deployed in enterprise and SMB networks. Administrators are urged to apply the updates immediately to prevent network compromise via the UniFi management plane.

Attack Type : Remote unauthenticated exploitation

Cause of Issue : Multiple critical flaws

Takeaway : Network infrastructure devices, especially those used in large fleets, are high-value targets for remote compromise.

Compliance Corner

Navigating SEBI's AI Mandates

On May 5, 2026, SEBI issued circular No. HO/13/19/12(1)2026-ITD1_CIMGI/10873/2026, addressing the risks of AI-driven vulnerability tools. SEBI warns that while these tools offer speed, they enable rapid, large-scale reconnaissance by malicious actors.

Furthermore, the mandate emphasizes the critical need for validating AI outputs to prevent dangerous misconfigurations and protect the wider market ecosystem from systemic, cascading vulnerabilities.

Action Required

To align with the cyber-suraksha.ai initiative, your organization must :

Update Protocols

Integrate your security operations with the cyber-suraksha.ai reporting framework.

Document Risk

Create mitigation strategies specifically for AI-related data leakage and output reliability.

Audit Vendors

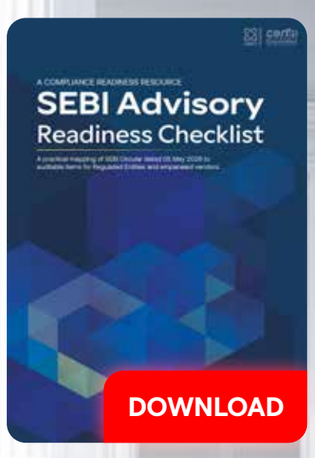
Enforce rigorous security reviews for any third-party providers using AI-assisted scanners.

Map AI Assets

Audit all AI-based security and scanning tools currently in your infrastructure.

Compliance Self-Assessment Checklist

Are you prepared to meet these new regulatory expectations? Use our interactive checklist to verify your organization's adherence to the latest circular.



9. Showboat Linux Malware Hits Telecom

On May 21, 2026, Lumen Technologies' Black Lotus Labs disclosed Showboat, a modular post-exploitation Linux framework used since at least mid-2022 against a Middle East telecom provider. The malware can spawn a remote shell, transfer files, and act as a SOCKS5 proxy. Researchers link it to a China-aligned cluster, with C2 nodes in Chengdu, Sichuan. Calypso, active since 2016, is a suspected operator, with overlaps to PlugX, ShadowPad, and NosyDoor frameworks.

Attack Type : Linux backdoor with SOCKS5 proxy

Cause of Issue : Targeted telecom intrusion

Takeaway : Specialized modular malware frameworks are used in long-term surveillance against telecom infrastructure.

10. Quasar Linux Rootkit Targets Systems

BleepingComputer reported on May 5, 2026 a previously undocumented Linux implant named Quasar Linux (QLNX) targeting developers' systems with rootkit, backdoor, and credential-stealing capabilities. The implant blends into normal developer and application behavior, evading endpoint protection. The campaign shows supply-chain-focused threat actors increasingly building tooling targeting identities and automation systems in modern software delivery pipelines.

Attack Type : Rootkit and credential theft

Cause of Issue : Targeted developer intrusion

Takeaway : Supply-chain-focused actors are developing implants exploiting identities and automation in developer environments.

Enterprise Applications & Collaboration Tools

11. MuddyWater Teams False Flag Attack

The Iranian state-sponsored group MuddyWater (aka Mango Sandstorm, Seedworm, Static Kitten) was attributed by Rapid7 in May 2026 to a ransomware attack that masqueraded as a Chaos ransomware-as-a-service operation. Attackers used Microsoft Teams social engineering to gain initial access, stole credentials, exfiltrated data, and established persistence, prioritizing intelligence collection over encryption. The activity highlights the convergence of state-sponsored espionage with cybercriminal RaaS tradecraft to obscure attribution.

Attack Type : False flag ransomware

Cause of Issue : Social engineering via Teams

Takeaway : State-sponsored actors are increasingly adopting cybercriminal tradecraft to obscure the true intent of their operations.

12. Facebook Accounts Hacked via Google

A Vietnamese-linked operation used Google AppSheet to create high-legitimacy phishing relays targeting Facebook Business accounts, leading to 30,000 account takeovers. By abusing the trust associated with a legitimate Google service, the attackers effectively bypassed email filters to distribute convincing lures. The stolen accounts were then sold on illicit marketplaces. This case is a stark reminder of how enterprise-trusted platforms are repurposed as delivery and monetization layers by threat actors for mass-scale fraud.

Attack Type : Phishing and account takeover

Cause of Issue : Abuse of Google service

Takeaway : Attackers are successfully weaponizing trusted cloud platform features to bypass email filters and deceive users.

APT Espionage & Emerging Attack Techniques

13. Cisco Workload Flaw Grants Admin

A maximum-severity privilege escalation vulnerability in Cisco Secure Workload allowed attackers to gain administrative access. By exploiting insufficient validation on REST API endpoints, an unauthenticated attacker could take control of the cluster software. Secure Workload acts as a control plane for visibility and policy enforcement. Cross-tenant access and ability to modify security policy makes this flaw a top priority for remediation in data center environments.

Attack Type : Privilege escalation

Cause of Issue : Improper authorization

Takeaway : Improper authorization checks in cloud-integrated management platforms can give attackers full control over workloads.

14. Microsoft Takes Down Fox Tempest

On May 19, 2026, Microsoft announced it had disrupted a malware-signing-as-a-service (MSaaS) operation run by Fox Tempest, which sold signed binaries using fraudulently obtained code-signing certificates. The service disguised malware as legitimate software like AnyDesk, Microsoft Teams, PuTTY, and Cisco Webex for $5,000–$9,000 per signing. It enabled deployment of Rhysida, Akira, INC, Qilin, and BlackByte ransomware by groups including Vanilla Tempest and Storm clusters.

Attack Type : Code-signing abuse

Cause of Issue : Certificate fraud

Takeaway : Adversaries are monetizing the abuse of trusted code-signing infrastructure to bypass security controls.

15. China UAT-8302 Deploys FINALDRAFT

A sophisticated China-nexus group targeted government entity in South America and Europe using a suite of custom backdoors like NetDraft and FINALDRAFT to maintain long-term espionage. The group utilized modular reconnaissance and lateral movement tools, often shared among other China-linked threat clusters. By maintaining a presence on high-value government endpoints, they sought persistent access for data exfiltration. This illustrates the high degree of coordination and tool-sharing among advanced threat actors.

Attack Type : APT espionage custom backdoors

Cause of Issue : Targeted intrusion

Takeaway : Close cooperation among Chinese threat clusters leads to sharing of sophisticated modular tooling that is difficult to detect.

16. VENOMOUS#HELPER Phishing Hits Orgs

Attackers targeted over 80 U.S. organizations by using phishing to deploy legitimate Remote Monitoring and Management (RMM) software, allowing for persistent, hands-on intrusions. The campaign leveraged RMM tools like SimpleHelp and ScreenConnect to maintain clandestine access, mimicking the administration patterns of managed service providers. The use of these powerful, legitimate tools highlights the challenge for defenders in distinguishing between authorized management activity and malicious, long-term persistence.

Attack Type : RMM tool abuse

Cause of Issue : Phishing with legitimate software

Takeaway : Living-off-the-land techniques using legitimate RMM tools are a preferred method for maintaining long-term, undetected access.

A Journey of Expertise with

JERRY

We are proud to celebrate a journey of growth and dedication at Briskinfosec. This month, we shine our spotlight on Jerry, a valued leader who has been an integral part of our organization for over seven years.

Jerry's career at Briskinfosec is defined by his relentless curiosity and a passion for cybersecurity. Over the years, he has navigated the complexities of our industry, consistently rising to every challenge and deepening his technical expertise. Recently, he further solidified his professional prowess by successfully completing his OSWE Offensive Security Web Expert certification. Through continuous learning and an unwavering commitment to our mission, he has become a cornerstone of our technical operations.

His path is more than just a professional milestone; it is a testament to the culture we cultivate at Briskinfosec. We foster an environment that empowers individuals to evolve, lead, and shape the future of our security practice. We are honored to have Jerry driving our team toward excellence, and we look forward to many more years of his leadership and success.

"Briskinfosec has been more than a workplace; it has been the foundation of my professional identity. This is a place that offers true freedom to innovate and explore new security frontiers. The culture here challenges you to constantly push boundaries, and having the mentorship to grow here is a privilege."

Jerry Louis

Lead - Cyber Security Research

17. Pwn2Own Berlin 2026 Awards $1.3M

A major hacking contest saw researchers demonstrate 47 zero-day exploits against browsers, enterprise software, and LLMs, showing the depth of unpatched flaws in common tech. These findings highlighted the efficacy of chaining multiple, individually less severe vulnerabilities to achieve system compromise. The event serves as a reminder of the vast ecosystem of undiscovered bugs and the ingenuity of security researchers, which threat actors are likely replicating for attack chains.

Attack Type : Zero-day demonstrations

Cause of Issue : Multiple chained flaws

Takeaway : Complex logic bug chaining remains an effective and rewarded method for compromising hardened software stacks.

18. MiniPlasma Zero-Day Grants SYSTEM

Proof-of-concept code was released for an unpatched Windows privilege escalation vulnerability in the Cloud Filter driver affecting fully updated systems. The flaw impacts cldflt.sys and its HsmOsBlockPlaceholderAccess routine, originally reported to Microsoft by Google Project Zero's James Forshaw in September 2020 as CVE-2020-17103. The issue remains unpatched, and BleepingComputer confirmed the PoC works against fully updated Windows 11 Pro on May 2026 Patch Tuesday updates.

Attack Type : Privilege escalation

Cause of Issue : Unpatched 2020 flaw regression

Takeaway : Regressions (re-emergence of old bugs) can leave even fully patched systems vulnerable to high-privilege attacks.

Vulnerabilities & CVE Disclosures

19. GreenPlasma YellowKey Zero-Day PoCs

Researcher Chaotic Eclipse (Nightmare Eclipse) published in May 2026 proof-of-concept exploits for two new unpatched Microsoft Windows vulnerabilities named YellowKey and GreenPlasma - a BitLocker bypass and a privilege-escalation flaw, respectively. The BitLocker bypass functions like a backdoor as the vulnerable component is present only in the Windows Recovery Environment (WinRE), used to repair boot-related issues. The disclosures follow the researcher's earlier release of BlueHammer and RedSun.

Attack Type : BitLocker bypass and LPE

Cause of Issue : Unpatched WinRE component

Takeaway : The release of public PoC code rapidly increases the likelihood of active, wide-scale exploitation by threat actors.

20. Cisco SD-WAN Auth Bypass Zero-Day

A maximum-severity (CVSS 10.0) authentication bypass flaw in Cisco Catalyst SD-WAN Controller (CVE-2026-20182) was actively exploited in zero-day attacks to gain administrative privileges. The vulnerability is in the vdaemon DTLS service on UDP port 12346 and lets an unauthenticated remote attacker become an authenticated peer of the target appliance. CISA added the flaw to KEV on May 14 and ordered federal agencies to patch within three days, by May 17, 2026.

Attack Type : Authentication bypass

Cause of Issue : Broken peer authentication

Takeaway : Critical infrastructure flaws in network management planes are actively exploited in the wild, requiring emergency patching.

21. PAN-OS User-ID Portal Zero-Day RCE

A critical buffer overflow in the Palo Alto Captive Portal allowed unauthenticated remote attackers to execute code as root on internet-facing firewalls. The vulnerability provided a direct path to the underlying operating system, granting attackers total control. Because these firewalls guard the perimeter of sensitive networks, the impact was catastrophic. The incident underscored the danger of internet-exposed security appliances with memory corruption flaws in management interfaces.

Attack Type : Remote code execution

Cause of Issue : Buffer overflow

Takeaway : Internet-exposed security appliances are top-tier targets; vulnerabilities require immediate remediation due to high risk.

22. Ivanti EPMM CVE-2026 Zero-Day RCE

A critical remote code execution vulnerability in Ivanti Endpoint Manager Mobile allowed attackers with administrative privileges to execute arbitrary code on appliances. The flaw, exploited in the wild, was severe enough that CISA mandated a four-day patching window for federal agencies. EPMM manages mobile device policies and sensitive configuration data, so control of the appliance could lead to significant downstream security failures. This highlights risk in management infrastructure.

Attack Type : Remote code execution

Cause of Issue : Improper input handling

Takeaway : Aggressive federal patching deadlines highlight zero-day exploitation severity

23. Exchange Server CVE-2026 Exploited

Microsoft disclosed CVE-2026-42897 (CVSS 8.1), an actively exploited cross-site scripting and spoofing flaw in on-premises Exchange Server 2016, 2019 and Subscription Edition. Attackers send a specially crafted email that, when opened in Outlook Web Access under certain interaction conditions, can execute arbitrary JavaScript in the browser context. Microsoft released Exchange Emergency Mitigation Service (EEMS) mitigations. This highlights the persistent risk of web-based attacks on legacy email infrastructure.

Attack Type : Cross-site scripting and spoofing

Cause of Issue : Improper input neutralization

Takeaway : Email infrastructure remains a high-value, vulnerable target requiring immediate application of emergency mitigations.

24. Microsoft May 2026 Fixes 120 Flaws

Microsoft's May 2026 Patch Tuesday delivered security updates for 120 flaws, addressing 17 Critical vulnerabilities — 14 remote code execution, 2 elevation of privilege, and 1 information disclosure. Notable bugs include CVE-2026-35421 (Windows GDI RCE via malicious EMF files) and CVE-2026-41096 (Windows DNS Client RCE via crafted DNS responses). Many Microsoft Office, Word and Excel flaws were exploitable via the preview pane, prompting Microsoft to recommend immediate updates.

Attack Type : Remote code execution

Cause of Issue : Multiple memory, parsing flaws

Takeaway : Routine maintenance is essential; memory parsing flaws in common applications are the focus of monthly patch cycles.

25. Microsoft Mitigation for BitLocker Bypass

A security feature bypass vulnerability allowed local attackers to bypass BitLocker drive encryption, exposing sensitive data on protected drives. The flaw exists in the Windows Recovery Environment, allowing disk access when the system is in a troubleshooting state. Microsoft provided mitigation guidance as the flaw remained unpatched for some time after disclosure. This shows that strong encryption can be bypassed by weaknesses in recovery environment identity validation.

Attack Type : Security feature bypass

Cause of Issue : BitLocker validation flaw

Takeaway : Encryption is not a silver bullet; flaws in implementation can allow attackers to bypass protection even on fully encrypted volumes.

26. Trend Micro Apex One Zero-Day Exploit

An exploited directory traversal flaw in Apex One allowed local attackers to inject malicious code deployed to all managed agents. The vulnerability let an attacker with lower-level access to the management server write arbitrary files, leading to code execution across the enterprise. This demonstrates the extreme risk of management platforms; a single vulnerability can compromise an entire fleet of endpoints, giving attackers control over the security environment.

Attack Type : Directory traversal

Cause of Issue : Improper path validation

Takeaway : Compromising management servers allows attackers to push malicious updates to enterprise agent fleet, maximizing impact.

27. DirtyDecrypt Linux Kernel LPE PoC

Proof-of-concept exploit code was published in May 2026 for DirtyDecrypt (aka DirtyCBC), a Linux kernel local privilege escalation flaw tracked as CVE-2026-31635. Discovered by the Zellic and V12 security team on May 9, 2026, the bug is an rxgk pagecache write caused by a missing copy-on-write guard in rxgk_decrypt_skb. Maintainers had previously patched a duplicate in the mainline kernel. The PoC was published on GitHub, raising the risk of widespread exploitation.

Attack Type : Local privilege escalation

Cause of Issue : Missing copy-on-write guard

Takeaway : Kernel vulnerabilities remain critical, and release of PoC code lowers barrier for attackers to gain root access.

28. KnowledgeDeliver LMS Flaw Exploited

Threat actors exploited a zero day vulnerability in Digital Knowledge KnowledgeDeliver LMS to achieve unauthenticated remote code execution through ASP.NET ViewState deserialization (CVE-2026-5426). Attackers deployed the Godzilla web shell, modified JavaScript files, displayed fake security plugin alerts, and infected users with Cobalt Strike Beacon payloads. This highlights the danger of shared deployment templates, as a single compromised key can endanger an entire ecosystem of installations.

Attack Type : RCE, Web Shell, Malware

Cause of Issue : ASP.NET machine keys web.config

Takeaway : Reused/hardcoded keys in enterprise software templates create systemic vulnerabilities exploitable across many instances.

Monthly Intelligence Spotlight

1. CERT-In's New Advisory on AI-Driven Cyber Risks

CERT-In warns that AI-powered attackers can weaponize vulnerabilities within hours, not weeks. Discover the 30-day action plan and 24-hour patch strategy organizations need to stay ahead of AI-driven cyber threats.

Read More

2. Inside Claude Mythos and What the Indian Defender Actually Needs to Know

AI models like Claude Mythos are reshaping cyber warfare by accelerating vulnerability discovery and exploit creation. Learn why traditional security timelines are collapsing and what defenders must do next.

Read More

3. The Cyber Capability Gap Between Mythos, GPT-5.5 and Open-Weight Models Explained

The real cybersecurity risk is not the most powerful AI model but the most accessible one. Explore how Mythos, GPT 5.5, and open weight models differ and why accessibility matters more than capability.

Read More

Cyber resilience is built before the incident, not during it.

BriskInfosec

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