THREATSPLOIT

ADVERSARY REPORT

BriskInfosec™
VULNERABILITY TO VICTORY

www.briskinfosec.com

91st Edition
Mar 2026

DEAR READERS,

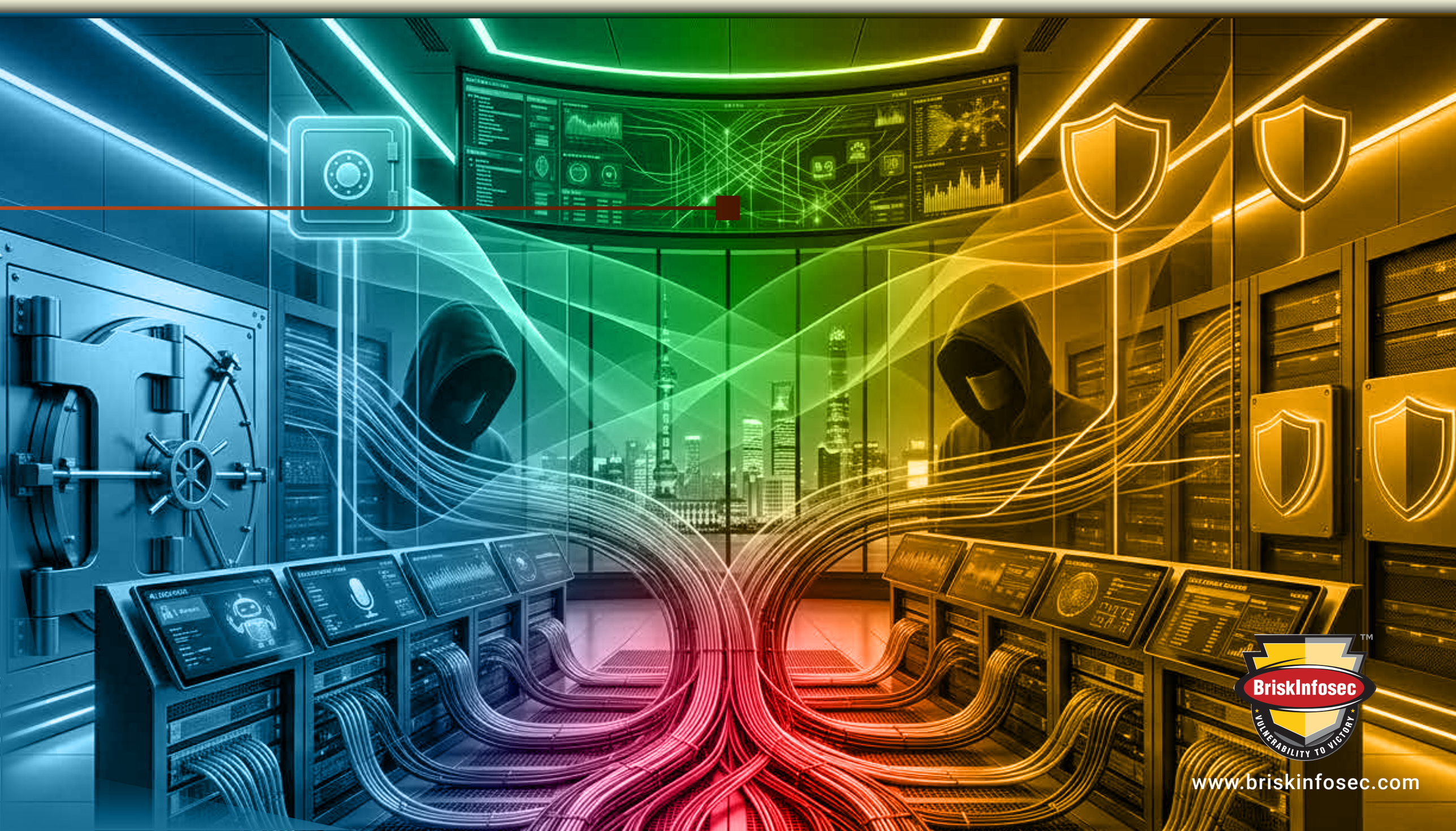
Modern offices are humming with efficiency as we hand over our routines to digital assistants and automated systems. It is an exciting era of growth, but in the rush to innovate, we often overlook the invisible digital threads that weave our organizations together. These connections create complex layers that are increasingly difficult to manage.

While we see seamless productivity, the adversary sees a landscape of unexplored shadows. Moving away from the loud strikes of the past, today's threat actors blend into the background of the workday. By following the very connections built for convenience, they can sit patiently inside a network. They wait for the perfect moment to act without ever raising an alarm or appearing as a threat.

This edition serves as your intelligence briefing to help you navigate this environment with confidence. We have curated the most significant developments to show exactly how the threat landscape is evolving. Beyond raw data, this report helps your team understand the logic behind modern intrusions so you can stay ahead of those who thrive on silence and stealth.

True resilience is built on constant awareness. It is vital to treat every automated system and digital identity with the same level of oversight you provide to your most trusted staff members. By remaining proactive and carefully monitoring the flow of information, you ensure your organization stays secure while continuing to lead in a connected world.

- Briskinfosec Threat Intelligence Team



APT & NATION STATE ATTACKS

1.China Aligned UNC3886 Espionage in Telecom Sector

A China linked advanced persistent threat group tracked as UNC3886 breached the largest telecom providers in Singapore through a targeted cyber espionage campaign. Attackers used an undisclosed zero day exploit to bypass perimeter defenses and deployed rootkits for long term persistence. Authorities confirmed limited access to critical systems but reported no service disruption or customer data theft. The incident triggered a national level response operation to protect other infrastructure sectors.

Attack Type : APT Espionage

Cause of Issue : Zero Day Vulnerability and Advanced Rootkit Deployment

Takeaway : Harden telecom perimeters and monitor for unauthorized rootkit activity

2. Shadow Campaigns: Global Intelligence Gathering (TGR STA 1030)

A state sponsored threat actor tracked as TGR STA 1030 conducted global cyber espionage operations called Shadow Campaigns, targeting government and critical infrastructure across 155 countries. The group compromised at least 70 organizations using phishing, vulnerability exploitation, and a custom Linux rootkit named ShadowGuard. The campaign focused on strategic intelligence gathering, using advanced stealth techniques and infrastructure blending to evade detection by standard security tools.

Attack Type : APT Espionage

Cause of Issue : Phishing Exploitation and Custom Linux Rootkits

Takeaway : Implement advanced Linux endpoint monitoring to detect eBPF rootkits

3. Iran Linked Infy Relaunches Tornado Malware Framework

The Iranian cyber espionage group Infy resumed operations after an internet blackout by deploying new command and control infrastructure and updating its Tornado malware framework. The latest variants use domain generation algorithms and Telegram APIs for covert communications. Researchers also observed exploitation of a recent WinRAR vulnerability to deliver payloads. The campaign focuses on targeted intelligence gathering against individuals and organizations, reinforcing their long-term goals.

Attack Type : APT Espionage

Cause of Issue : Use of WinRAR Exploits and Covert Telegram C2

Takeaway : Patch WinRAR and monitor for unusual Telegram API traffic patterns

4. Bloody Wolf Spear Phishing Abuses Legitimate Remote Tools

The threat actor Bloody Wolf launched spear phishing campaigns targeting government and finance sectors using malicious PDF lures to deploy the NetSupport remote access trojan. The malware installs persistence through scheduled tasks and registry changes, enabling long term remote control and data theft. Researchers believe the group is motivated by both financial gain and espionage style surveillance. The use of legitimate remote support tools allows them to blend in with normal administrative work.

Attack Type : Spear Phishing / Remote Access

Cause of Issue : User Execution of Malicious PDF Lures

Takeaway : Block unauthorized remote support tools and audit scheduled tasks

MALWARE, RATS & BOTNETS

5. ZeroDayRAT: Commercial Mobile Spyware Targeting iOS and Android

ZeroDayRAT is a commercial mobile spyware platform advertised on Telegram that provides attackers with full remote control of infected devices. The malware supports surveillance, credential theft, and real time tracking. Operators can activate cameras, microphones, and screen recording, while also capturing SMS messages and user input. Researchers warn that compromised mobile devices may expose enterprise data and allow attackers to move laterally into internal corporate environments quite easily.

Attack Type : Mobile Spyware / Espionage

Cause of Issue : Installation of Malicious Apps from Unofficial Sources

Takeaway : Use Mobile Device Management to prevent unofficial app installations

6. Crazy Ransomware Affiliates Abuse Monitoring Software

Researchers observed a ransomware affiliate abusing legitimate employee monitoring software and remote support tools to maintain persistence and prepare for deployment. The attackers installed professional monitoring clients to gain interactive access and blend malicious activity with normal administration workflows. This demonstrates a growing ransomware tactic of leveraging trusted remote management software instead of traditional malware to avoid detection by standard endpoint security tools.

Attack Type : Ransomware / Persistence

Cause of Issue : Abuse of Legitimate Employee Monitoring Software

Takeaway : Audit all remote support software and restrict its use to admins

7. SSHStalker Botnet Revives IRC Infrastructure for Control

Researchers uncovered a new Linux botnet named SSHStalker that uses old school IRC infrastructure for command and control operations. The malware spreads by scanning for exposed SSH services and brute forcing credentials. Once infected, systems connect to hard coded IRC channels and remain mostly idle, suggesting attackers are hoarding access for future campaigns. The botnet also includes cryptomining modules, cloud credential harvesting tools, and distributed denial of service capabilities.

Attack Type : Botnet Malware

Cause of Issue : Weak SSH Credentials and Exposed Services

Takeaway : Enforce strong SSH keys and disable password-based authentication

8. Trojanized 7 Zip Installer Enrolls PCs into Proxy Networks

Threat actors created a fake download site distributing a trojanized installer for 7 Zip bundled with a hidden proxy tool. Victims believe they are installing legitimate archiving software, but the malware silently enrolls their device into a residential proxy network. This allows attackers to route malicious traffic through compromised machines to hide their true location. The campaign relies on SEO poisoning and lookalike domains to trick users searching for common utility software downloads.

Attack Type : Trojan Installer / Proxy Hijacking

Cause of Issue : Typosquatting and Malicious SEO Poisoning

Takeaway : Only download software from official verified developer websites

9. AISURU Kimwolf Botnet Sets Global Record for DDoS Volume

The AISURU Kimwolf botnet launched a record-breaking distributed denial of service attack peaking at 31.4 Tbps. The hyper volumetric attack lasted only about 35 seconds but demonstrated massive scale powered largely by compromised IoT and Android devices. Security providers mitigated the attack automatically, highlighting how modern botnets are shifting toward extremely short but devastating network floods capable of overwhelming infrastructure before traditional response measures activate.

Attack Type : DDoS Botnet

Cause of Issue : Mass Compromise of Unsecured IoT and Android Devices

Takeaway : Secure IoT devices and implement automated DDoS mitigation tools

10. TeamPCP Worm Automates Cloud API and Container Exploitation

Researchers uncovered a large-scale worm driven campaign targeting exposed cloud native services such as Docker APIs and Kubernetes clusters. The operation uses misconfigurations and known vulnerabilities to compromise infrastructure, deploy proxy networks, and launch follow on attacks like ransomware. Instead of targeting specific industries, attackers focus on vulnerable cloud resources to build a scalable criminal ecosystem. This highlights the risk of leaving cloud management dashboards exposed.

Attack Type : Cloud Worm / API Exploitation

Cause of Issue : Cloud Misconfigurations and Exposed Management APIs

Takeaway : Use strong authentication and private networks for cloud APIs

11. Operation Aether Targets Phobos Ransomware Ecosystem

Authorities arrested a suspect tied to the Phobos ransomware ecosystem during an international law enforcement operation called Operation Aether. Investigators seized devices containing stolen credentials and server access data used to support ransomware intrusions. The suspect allegedly communicated with operators using encrypted messaging platforms to coordinate attacks. The operation is part of a broader effort to dismantle the long running ransomware as a service network used by global criminals.

Attack Type : Ransomware / Law Enforcement Action

Cause of Issue : Ransomware Affiliate Infrastructure Access

Takeaway : Monitor for Phobos indicators and maintain offline data backups

WEB, BROWSER & AI SECURITY

12. Malicious Chrome Extensions Hijacking AI Session Tokens

Researchers uncovered multiple malicious Chrome extensions designed to inject affiliate tags and extract ChatGPT authentication tokens. Some add ons modify e commerce links to redirect commissions, while others target AI workflows by injecting scripts into specific domains to capture session tokens. Additional extensions harvest cookies and manipulate clipboard access. This highlights how browser extensions are becoming a major attack surface for gaining persistent access to cloud accounts.

Attack Type : Credential Theft / AI Hijacking

Cause of Issue : Malicious Browser Extensions and Script Injection

Takeaway : Restrict browser extensions to an approved enterprise whitelist

13. Google Warns of AI Augmentation in State Backed Operations

Google reported that multiple state backed threat actors are using the Gemini AI model to support nearly every phase of cyber operations. Attackers leverage the AI for reconnaissance, phishing development, and malware coding. The report highlights growing AI augmentation rather than full automation, showing how adversaries integrate generative AI into existing toolchains to accelerate their operations. This allows them to significantly improve the success rates of their social engineering.

Attack Type : AI Assisted Attacks

Cause of Issue : Misuse of Generative AI for Phishing and Reconnaissance

Takeaway : Use AI based defenses to counter AI generated phishing lures

14. JokerOTP Phishing Platform Dismantled by Dutch Authorities

Authorities arrested a suspect behind the JokerOTP phishing platform, which was designed to capture multi factor authentication codes through automated voice phishing. The platform enabled attackers to impersonate legitimate services and trick victims into entering codes during live login attempts. Over two years, the operation caused millions in losses and targeted major platforms like PayPal and Apple. This shows the scale of the professional phishing as a service ecosystem today.

Attack Type : OTP Phishing / MFA Bypass

Cause of Issue : Automated Social Engineering and Voice Phishing

Takeaway : Educate users that support staff will never ask for OTP codes

15. OpenClaw AI Agent Introduces Enterprise RCE Risks

OpenClaw is an autonomous open source AI agent capable of executing commands and integrating with enterprise platforms. Rapid adoption triggered multiple security incidents including exposed deployments leaking credentials and a critical remote code execution vulnerability. The crisis highlights how AI agents with persistent memory and elevated integrations can become high impact insider threats if they are misconfigured. This creates a new and unmonitored attack surface for modern companies.

Attack Type : Agent Abuse / Remote Code Execution

Cause of Issue : Exposed AI Agents and Vulnerable Plugin Logic

Takeaway : Audit AI agent permissions and isolate them from sensitive data

16. Physical Phishing Letters Target Hardware Wallet Recovery Phrases

Threat actors launched a physical mail phishing campaign targeting cryptocurrency users by sending fake letters impersonating security notices from Trezor and Ledger. The letters instruct victims to scan QR codes that redirect to phishing sites requesting wallet recovery phrases. Once entered, attackers can import the wallet and steal all funds. The campaign uses urgency tactics such as mandatory authentication checks to pressure victims into complying with the fraudulent request.

Attack Type : QR Phishing / Physical Mail Social Engineering

Cause of Issue : Trust in Physical Mail and Seed Phrase Exposure

Takeaway : Never enter hardware wallet recovery phrases into any website

17. ClickFix Campaign Abuses Claude AI Artifacts for Malware

Threat actors abused publicly shared Claude AI artifacts and Google Ads to distribute ClickFix style malware targeting macOS users. Victims searching for technical tools were redirected to AI generated guides instructing them to paste malicious commands into the Terminal. Executing these commands installed an infostealer that captures keychain data and crypto wallets. This demonstrates how AI generated content is becoming a primary and trusted vector for new social engineering.

Attack Type : ClickFix Malware / AI Social Engineering

Cause of Issue : User Execution of Malicious Shell Commands from AI Guides

Takeaway : Prevent users from running Terminal commands found on the web

18. AiFrame Campaign: Malicious Extensions Harvesting Gmail Data

Researchers uncovered a campaign named AiFrame involving more than 30 malicious Chrome extensions posing as AI assistants. Installed by hundreds of thousands of users, the extensions steal browsing data and Gmail content by injecting scripts that read page data directly from the browser. Some extensions remain available in web stores and can remotely change their behavior to bypass review processes. This shows the persistent danger of unvetted browser tools in corporate settings.

Attack Type : Malicious Extensions / Data Theft

Cause of Issue : Deceptive Extensions and Extension Review Bypass

Takeaway : Audit browser activity for unauthorized data exfiltration scripts

AI in the Attack Chain

The New Digital Predator

Cybersecurity professionals once saw AI as the ultimate defense-spotting anomalies and reducing false positives at machine speed. But this technology has shifted the power balance. Every stage of the cyber kill chain now has an AI-augmented counterpart. This is no longer a projection, it is today's reality.

89% Surge in AI-enabled attacks, year-over-year

54% Click-through rate on AI-generated phishing lures

76% Of active malware rewrites its own code mid-execution

85% Of common passwords cracked by AI in under 10 seconds

Where attackers once needed time, AI compresses the cycle from reconnaissance to exfiltration into minutes. Large language models mimic legitimate emails with unnerving fluency. Generative image synthesis defeats visual verification, while adversarial learning deceives AI-driven defenses.

The New Arms Race

Organizations cannot rely on reactive security. Digital adversaries think, learn, and evolve in real time. Our posture must shift toward an AI versus AI confrontation, where defenders leverage machine learning for predictive detection and adaptive deception. Technology alone is not the answer. As systems become autonomous, accountability must evolve to ensure defense remains adaptive but never reckless.

The Human Element Remains Irreplaceable

In algorithmic warfare, the decisive advantage won't come from faster processors, but from the wisdom to integrate them responsibly. AI is both sword and shield. The real question is not how to stop it, but how to use wisely.

CRITICAL VULNERABILITIES & ZERO DAYS

19. Ivanti EPMM Zero Day Exploitation (CVE 2026 1281)

Ivanti has released emergency security updates for two critical Zero Day vulnerabilities in its Endpoint Manager Mobile platform. These specific flaws allow unauthenticated attackers to execute arbitrary code on affected appliances by exploiting deep weaknesses in the mobile device management infrastructure. Adversaries have been observed deploying web shells and accessing sensitive device information to move laterally within enterprise networks. Organizations with internet facing instances must assume compromise.

Attack Type : Remote Code Execution (RCE)

Cause of Issue : Unsanitized Code Injection in Management Interface

Takeaway : Rebuild impacted infrastructure and apply patches to all MDM servers

20. SmarterMail Critical Authentication Bypass (CVE 2026 24423)

SmarterTools recently issued urgent security updates for SmarterMail to fix a critical unauthenticated remote code execution flaw. The vulnerability allows attackers to execute arbitrary commands or hijack administrative accounts by abusing NTLM relay mechanisms and improper authentication checks. Multiple bugs were already exploited in the wild before the release of the latest build. Organizations running internet exposed mail servers are strongly advised to upgrade immediately and review their system logs.

Attack Type : Remote Code Execution (RCE)

Cause of Issue : Improper Authentication and NTLM Relay Vulnerability

Takeaway : Upgrade to SmarterMail Build 9511 and check for admin account hijack

21. Apple Zero Day dyld Memory Corruption (CVE 2026 20700)

Apple has released emergency updates to address a zero-day arbitrary code execution vulnerability in the dyld dynamic linker affecting the entire ecosystem. The flaw allows attackers with memory write capabilities to execute malicious code and has been used in highly sophisticated attacks against specific individuals. Because it was exploited alongside earlier web browser vulnerabilities in real world intrusions, users are urged to patch their devices immediately to prevent a full and silent system compromise.

Attack Type : Zero Day / Code Execution

Cause of Issue : Memory Corruption in Dynamic Linker

Takeaway : Update all iOS and macOS devices to the latest security version now

22. Windows Notepad Markdown Command Injection (CVE 2026 20841)

Microsoft fixed a high severity vulnerability in Windows Notepad that allowed remote code execution when users clicked specially crafted Markdown links. The flaw abused the Markdown rendering feature to launch executables or remote resources without displaying standard Windows security warnings. Attackers could embed malicious file protocol links inside Markdown files to enable silent program execution in the security context of the user. This shows how simple text editors become a primary attack vector.

Attack Type : Remote Code Execution (RCE)

Cause of Issue : Improper Sanitization of Markdown Links

Takeaway : Apply the latest Windows updates and be cautious with Markdown files

23. Fortinet FortiClientEMS SQL Injection RCE (CVE 2026 21643)

Fortinet has released security updates to fix a critical SQL injection vulnerability in FortiClientEMS that could allow unauthenticated attackers to execute arbitrary code through crafted HTTP requests. The flaw stems from improper input sanitization in SQL queries and carries a high severity rating for enterprise environments. While active exploitation was not confirmed at disclosure, organizations were urged to patch immediately because of the high risk of remote compromise and endpoint management data theft.

Attack Type : Remote Code Execution (RCE)

Cause of Issue : SQL Injection due to Improper Input Sanitization

Takeaway : Apply Fortinet security updates to the EMS server without delay

24. Dell RecoverPoint Hardcoded Credential Flaw (CVE 2026 22769)

A critical zero-day vulnerability in Dell RecoverPoint for Virtual Machines allows unauthenticated attackers to gain root level access through hardcoded credentials embedded in the management interface. This flaw has been actively exploited by a nation state threat cluster to deploy stealthy backdoors and pivot into internal infrastructure. Dell has released patches and urged immediate upgrades due to the maximum severity risk. This incident emphasizes the danger of static credentials in storage solutions.

Attack Type : Zero Day / Authentication Bypass

Cause of Issue : Use of Hardcoded Credentials in Management Software

Takeaway : Patch RecoverPoint immediately and audit for unauthorized root access

OPERATIONS & SUPPLY CHAIN

25. Open VSX Registry Attack Delivering GlassWorm Loader

Threat actors conducted a software supply chain attack on the Open VSX registry by compromising a legitimate developer account and publishing malicious updates to trusted extensions. The poisoned versions embedded the GlassWorm loader, which profiles systems and steals developer secrets. The attack leveraged stolen credentials and advanced hiding techniques to evade detection while silently distributing malware to many users. This highlights the risk to the entire developer ecosystem.

Attack Type : Supply Chain Compromise

Cause of Issue : Compromised Maintainer Credentials in Extension Registry

Takeaway : Use code signing and verify all third-party extension updates

26. eScan Antivirus Infrastructure Breach Distributes Trojanized Updates

Attackers breached eScan antivirus infrastructure and distributed malicious updates that replaced legitimate components with trojanized binaries. The attack delivered a multi stage PowerShell based malware chain designed to establish persistence and disable protections. The compromised updates were distributed for about two hours before detection and mainly affected systems in South Asia. This demonstrates a rare supply chain attack where trusted update mechanisms were abused.

Attack Type : Supply Chain Attack

Cause of Issue : Compromised Antivirus Update Server Infrastructure

Takeaway : Monitor for anomalous binary behavior even in trusted software

27. Conduent Breach Exposes Volvo Group Customer Information

Volvo Group confirmed that customer data was exposed following a cyberattack against its third-party service provider, Conduent. The breach impacted a benefits administration platform used to manage employee and customer related services. Attackers accessed personal information including names, addresses, and potentially financial data. The incident highlights ongoing risks from supply chain compromises where attackers target external vendors rather than the primary organization.

Attack Type : Data Breach / Third Party Compromise

Cause of Issue : Cyberattack on External Benefits Administration Vendor

Takeaway : Conduct regular security audits of all third-party service providers

28. dYdX Developer Libraries Compromised with Wallet Stealers

Researchers uncovered a software supply chain attack where legitimate dYdX developer packages on npm and PyPI were compromised and updated with malicious code. The trojanized versions stole cryptocurrency wallet seed phrases and device data, while the Python variant also deployed a remote access trojan. The poisoned updates were likely published using stolen maintainer credentials, specifically targeting developers building crypto trading tools and automation systems.

Attack Type : Supply Chain / Library Poisoning

Cause of Issue : Stolen Maintainer Credentials in Software Registries

Takeaway : Pin package versions and audit all new library updates manually

29. Evidence Driven SOC Workflows Accelerate Response Speed

Leading organizations are reducing analyst fatigue and improving response speed by adopting evidence driven SOC workflows. Instead of adding more tools, they use sandbox first investigations and automated triage to streamline incident analysis. These changes reduce decision fatigue and enable junior analysts to resolve alerts faster. The result is a lower mean time to respond and more sustainable operations, proving that strategic process changes are as vital as technical defenses.

Attack Type : Operational Strategy / SOC Optimization

Cause of Issue : Analyst Fatigue and High Alert Volume

Takeaway : Focus on automated triage to improve incident response efficiency

30. Tirith Tool: Defending Against Homoglyph Terminal Attacks

A new open source tool called Tirith helps defend against command line attacks that disguise malicious commands as safe ones using invisible characters or terminal injection tricks. It integrates into popular shells to analyze pasted commands before execution and block suspicious patterns like malicious payloads. The tool operates locally without sending data away and aims to reduce risks from modern social engineering techniques that specifically target developers and admins.

Attack Type : Command Injection / Social Engineering Defense

Cause of Issue : User Execution of Obfuscated Terminal Commands

Takeaway : Deploy Tirith to protect developers from malicious paste attacks

PRODUCT OVERVIEW

luraInsight

Offline SAST for Enterprise

Scan your source code for security vulnerabilities without ever sending a single line to the cloud. Enterprise-grade static analysis, fully offline, fully yours.

100%
OFFLINE
Your source code never leaves your environment ever.
ZERO DATA LEAKAGE

> ***"83% of applications contain at least one security flaw. Yet most enterprises still send their source code to third-party clouds for scanning. What if you didn't have to?"***

Core Capabilities

AI — AI-Powered Code Auditing

Leverages advanced AI to analyze source code in any programming language. Detects vulnerabilities with high accuracy no separate rule sets needed.

OFF — Fully Offline Operation

Runs entirely on-premises. Sensitive source code never leaves your network critical for banking, healthcare, defense, and government.

EXP — Export to PDF and XLS

Generate detailed scan reports in PDF and Excel. Share findings instantly with auditors, stakeholders, and development teams.

DSH — Complete Dashboard

Full-featured visual dashboard showing scan results, vulnerability severity, trend analysis, and guided remediatio all in one view.

Why LuraInsight Stands Out

Data Sovereignty, Guaranteed

Enterprises complying with GDPR, IRDAI, RBI, ISO 27001, or HIPAA cannot risk uploading source code to the cloud. LuraInsight eliminates this risk entirely.

Language-Agnostic Scanning

One tool, every language. The AI engine audits source code across all programming languages and frameworks without needing separate rule configurations.

LuraInsight vs. Traditional SAST Tools

Criteria	LuraInsight	Cloud SAST Tools
Source code privacy	**Code never leaves your network**	Uploaded to vendor servers
AI-powered analysis	**Built-in, language-agnostic AI**	Rule-based or limited AI
Internet dependency	**Zero (fully offline)**	Requires internet connection
Setup complexity	**Install and scan in minutes**	Weeks of configuration
Compliance alignment	**GDPR, IRDAI, RBI, ISO ready**	May conflict with data policies
Multi-language support	**Any language, one engine**	Separate plugins per language

sales@briskinfosec.com | www.briskinfosec.com

“ When risks remain unseen,
impact becomes inevitable,
Visibility changes the outcome.”

BriskInfosec™

VULNERABILITY TO VICTORY

sales@briskinfosec.com | www.briskinfosec.com