THREATSPLOIT

ADVERSARY REPORT

90th Edition
Feb 2026

BriskInfosec™
VULNERABILITY TO VICTORY

www.briskinfosec.com

Dear Readers,

Modern offices are humming with automation that helps us stay productive and efficient. It is an exciting era of growth where technology handles the heavy lifting while we focus on the big picture. However, in this rush to innovate, we often overlook the invisible digital threads that weave our entire organization together and create complex layers that are difficult to manage.

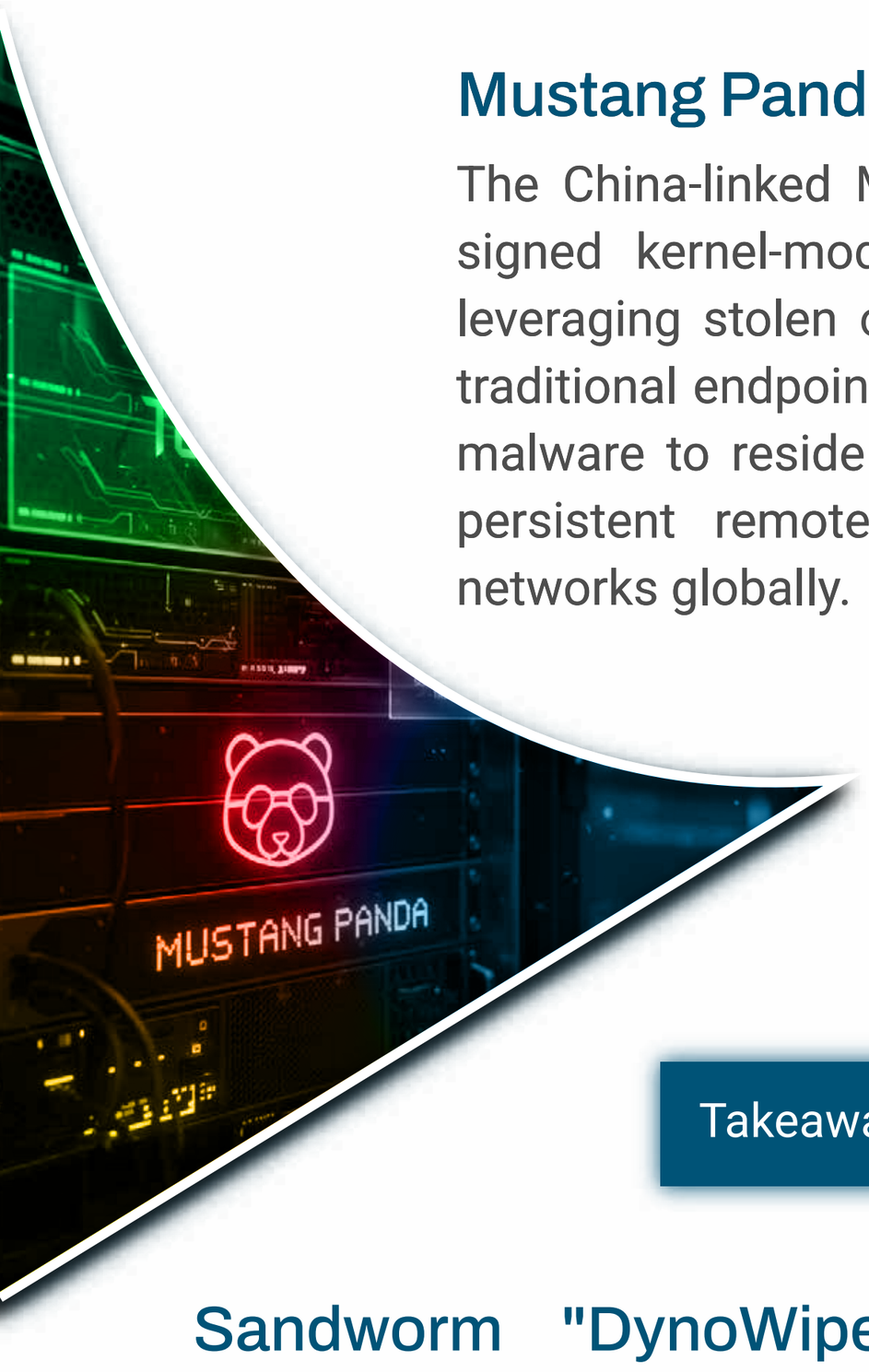
While we see a world of seamless productivity, the adversary sees a landscape of unexplored shadows and quiet corners. They have moved away from the loud strikes of the past and now choose to blend perfectly into the background of your normal workday. By following the very connections we built for convenience, they can sit patiently inside a network and wait for the perfect moment to act without ever raising an alarm.

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

True resilience is built on a culture of constant awareness and professional digital hygiene. 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 thrive in a connected world.

- Briskinfosec Threat Intelligence Team.

APT & Nation-State Attacks



Mustang Panda "ToneShell" Deployment via Signed Rootkits

The China-linked Mustang Panda APT has evolved its toolkit by utilizing a signed kernel-mode rootkit driver to deploy the ToneShell backdoor. By leveraging stolen or improperly issued digital certificates, the group evades traditional endpoint security controls that trust signed drivers. This allows the malware to reside at the kernel level, facilitating silent data exfiltration and persistent remote access within government and critical infrastructure networks globally.

Attack Type : APT

Causes : Abuse of Stolen Code-Signing Certificates

Takeaway : Implement strict driver-signing policies and audit kernel loads

Sandworm "DynoWiper" Attempt on Poland's Energy Infrastructure

Russia-aligned Sandworm (APT44) launched a destructive cyberattack targeting Poland's energy grid using a new wiper malware called DynoWiper. The adversary aimed to erase critical system data to disrupt power operations. Although defensive monitoring contained the impact, the incident underscores the threat of state-sponsored "wiper" operations designed for national sabotage rather than financial gain, particularly targeting infrastructure in strategically sensitive locations.

Attack Type : Wiper Attack

Causes : Nation-State Targeted Intrusion

Takeaway : Verify air-gapped backups and enhance OT threat hunting capabilities

Russia-Aligned APT Abuses Viber for Android Malware Distribution

A Russia-aligned threat group is spreading Android malware through malicious Viber messages containing links to poisoned APKs. Once installed, the malware requests extensive permissions to harvest SMS, contacts, and real-time location data. This campaign leverages the perceived trust of popular messaging platforms to bypass user suspicion and sideload applications outside official app stores, specifically targeting users in geopolitically sensitive regions for data collection.

Attack Type : Mobile Malware

Causes : Malicious Link Distribution via Trusted Apps

Takeaway : Educate users on the risks of sideloading APKs from messaging links

Transparent Tribe Deploys New Android RAT via Phishing Campaigns

The Transparent Tribe group is distributing a new Android remote access trojan (RAT) through WhatsApp and Telegram phishing. Victims are directed to fake app download pages for malicious APKs disguised as legitimate tools. Upon installation, the RAT gains permissions to monitor calls, exfiltrate device data, and capture ambient audio. This targeted social engineering campaign focuses on high-value groups to maintain persistent surveillance and gather intelligence from mobile devices.

Attack Type : Mobile RAT

Causes : Poisoned App Distribution (Phishing Links)

Takeaway : Enforce mobile device management (MDM) and block unverified APKs

North Korea-Linked Espionage Targets Critical Infrastructure

A North Korea-linked threat group is targeting industrial and critical infrastructure organizations using tailored malware and cyber espionage tactics. The campaign utilizes phishing, compromised websites, and custom remote access frameworks to infiltrate operational technology (OT) networks. Once inside, the group escalates privileges to exfiltrate sensitive engineering data, posing severe risks to the long-term integrity and operational continuity of essential national services.

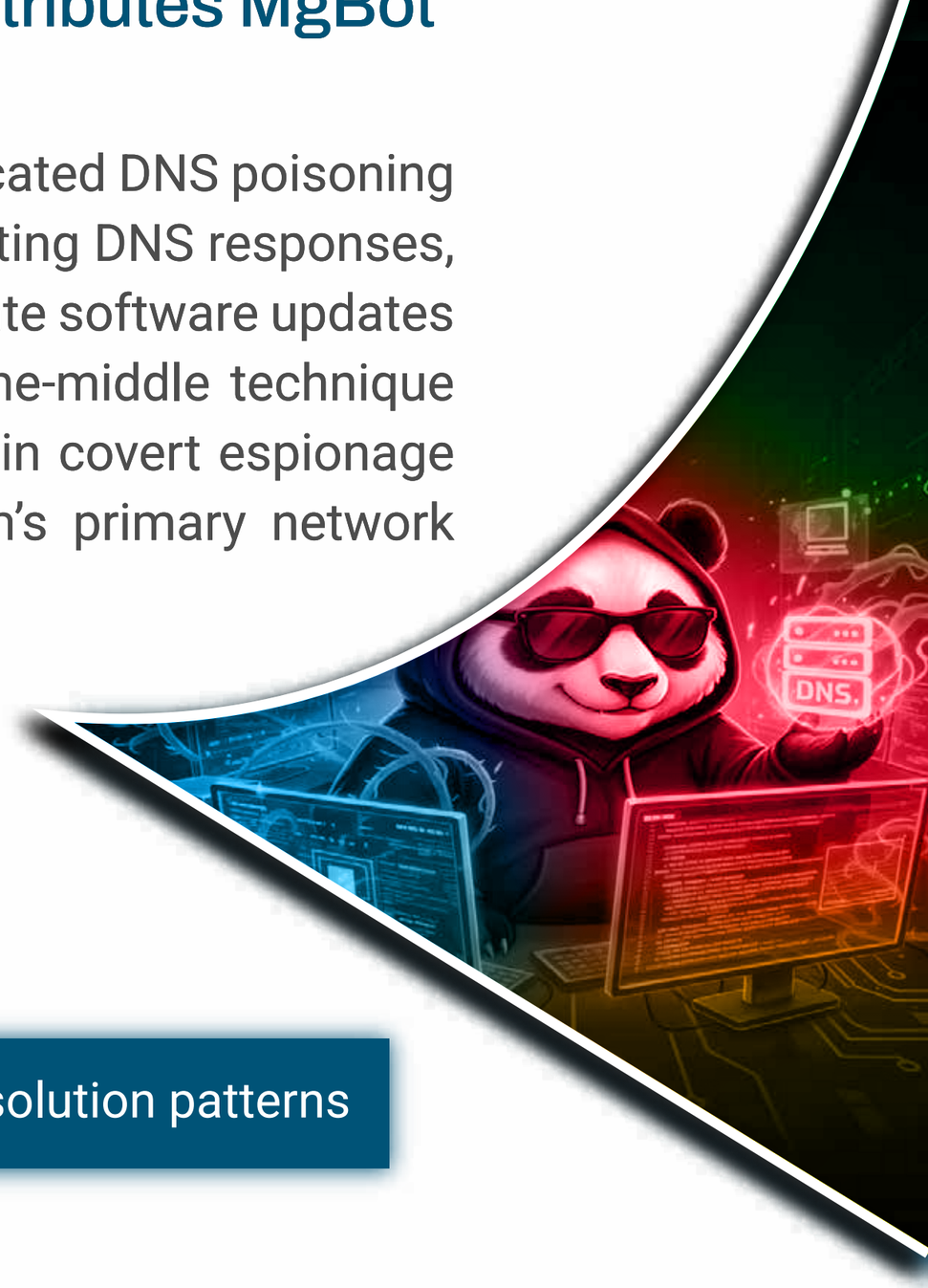
Attack Type : Malware

Causes : Phishing and Vulnerability Exploitation

Takeaway : Harden OT/IT boundaries and monitor for credential misuse in OT

Evasive Panda DNS Poisoning Campaign Distributes MgBot Backdoor

The China-linked APT Evasive Panda conducted a sophisticated DNS poisoning campaign to silently deliver its MgBot backdoor. By corrupting DNS responses, attackers pushed malicious payloads disguised as legitimate software updates to targets in India, Turkey, and China. This adversary-in-the-middle technique compromises network trust, allowing the group to maintain covert espionage operations without needing to directly breach the victim's primary network perimeter.



Attack Type : DNS Poisoning

Causes : Domain Response Manipulation

Takeaway : Deploy DNSSEC and monitor for anomalous DNS resolution patterns

UAT-7290 (China) Espionage Targeting Telecommunications Providers

The China-linked threat group UAT-7290 is targeting telecommunications providers across multiple regions using custom espionage malware and credential theft. The campaign utilizes spear-phishing and stolen certificates to infiltrate provider infrastructure and harvest sensitive subscriber data. The group focuses on long-term persistence and data collection, often abusing legitimate administrative tools ("living-off-the-land") to evade detection and maintain access to core network systems.

Attack Type : Espionage

Causes : Abuse of Administrative Tools and Certificates

Takeaway : Implement MFA for all admin tools and monitor certificate usage

MuddyWater "RustyWater" RAT Phishing Campaign

The Iran-linked MuddyWater group is deploying a new custom remote access trojan (RAT) dubbed RustyWater. Delivered via highly targeted phishing emails with weaponized attachments, the malware utilizes the Rust programming language to evade signature-based detection. Once executed, it provides the adversary with full command-line control and the ability to pivot laterally through the victim's network to identify and steal sensitive government data and strategic intelligence.

Attack Type : Phishing

Causes : Social Engineering and Weaponized Attachments

Takeaway : Train employees on document-based phishing and limit macro execution

OUR LATEST CYBER INSIGHTS

The Rise of Invisible Insider Threats

Explores how unsanctioned AI tools operating in the background can quietly move data, weaken controls, and turn regular employees into invisible insider risks, plus how to detect and govern this behaviour.

Read more

Measuring Cybersecurity ROI

Explains why classic ROI formulas fall short in security and shows how to prove value using resilience measures such as reduced downtime, faster recovery, and lower impact from cyber incidents.

Read more

Zero Trust Architecture

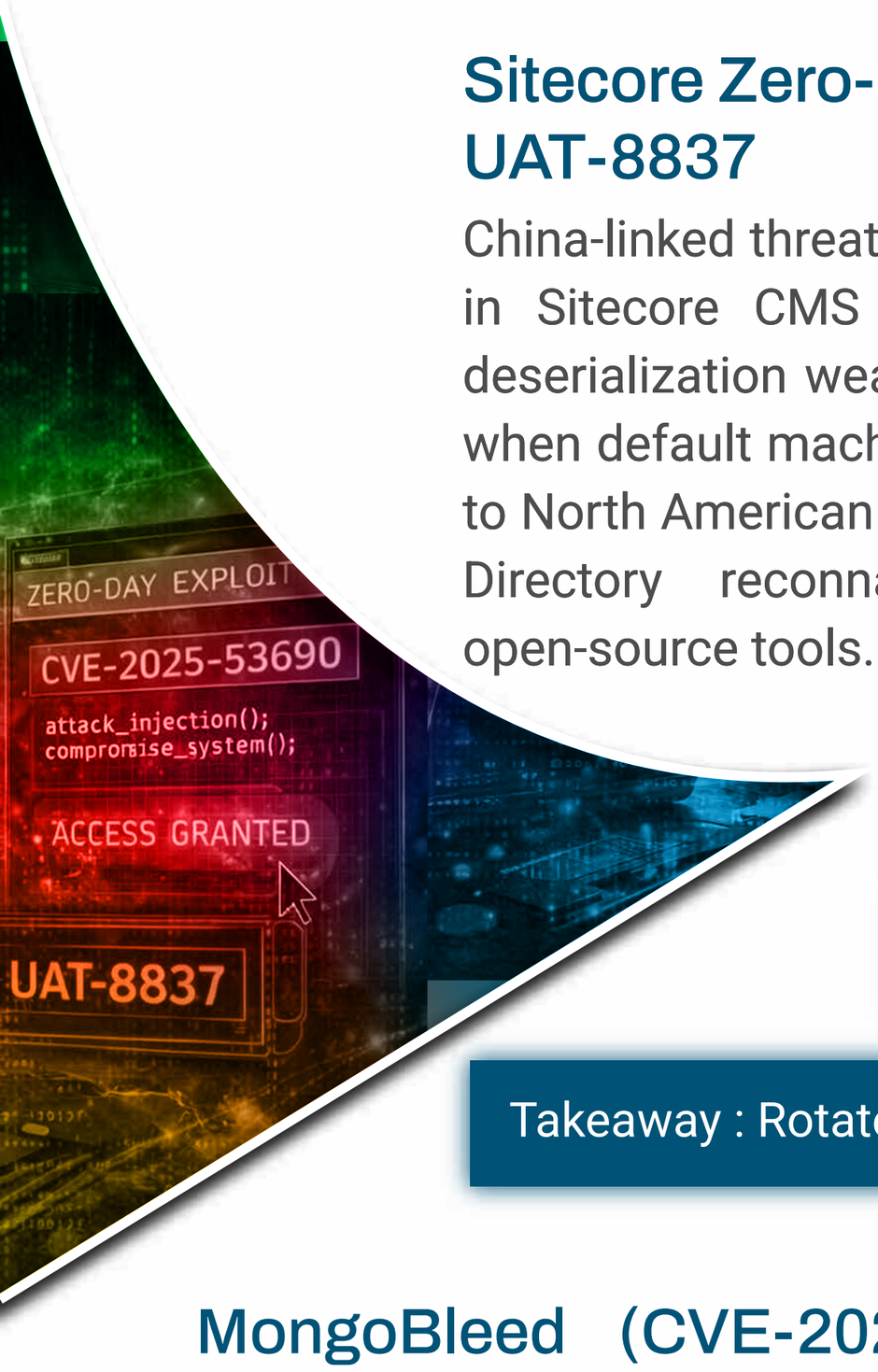
Describes how to evolve from perimeter-focused controls to a continuous, identity- and context-aware Zero Trust model that protects users, devices, and data wherever they operate.

Read more

BriskInfosec
VULNERABILITY TO VICTORY

www.briskinfosec.com

Critical Vulnerabilities & Zero-Days



Sitecore Zero-Day Exploitation (CVE-2025-53690) by UAT-8837

China-linked threat actor UAT-8837 is exploiting a critical zero-day vulnerability in Sitecore CMS (CVE-2025-53690). The flaw is rooted in a ViewState deserialization weakness that allows unauthenticated remote code execution when default machine keys are present. Adversaries use this for initial access to North American critical infrastructure, enabling credential harvesting, Active Directory reconnaissance, and persistent backdoor deployment via open-source tools.

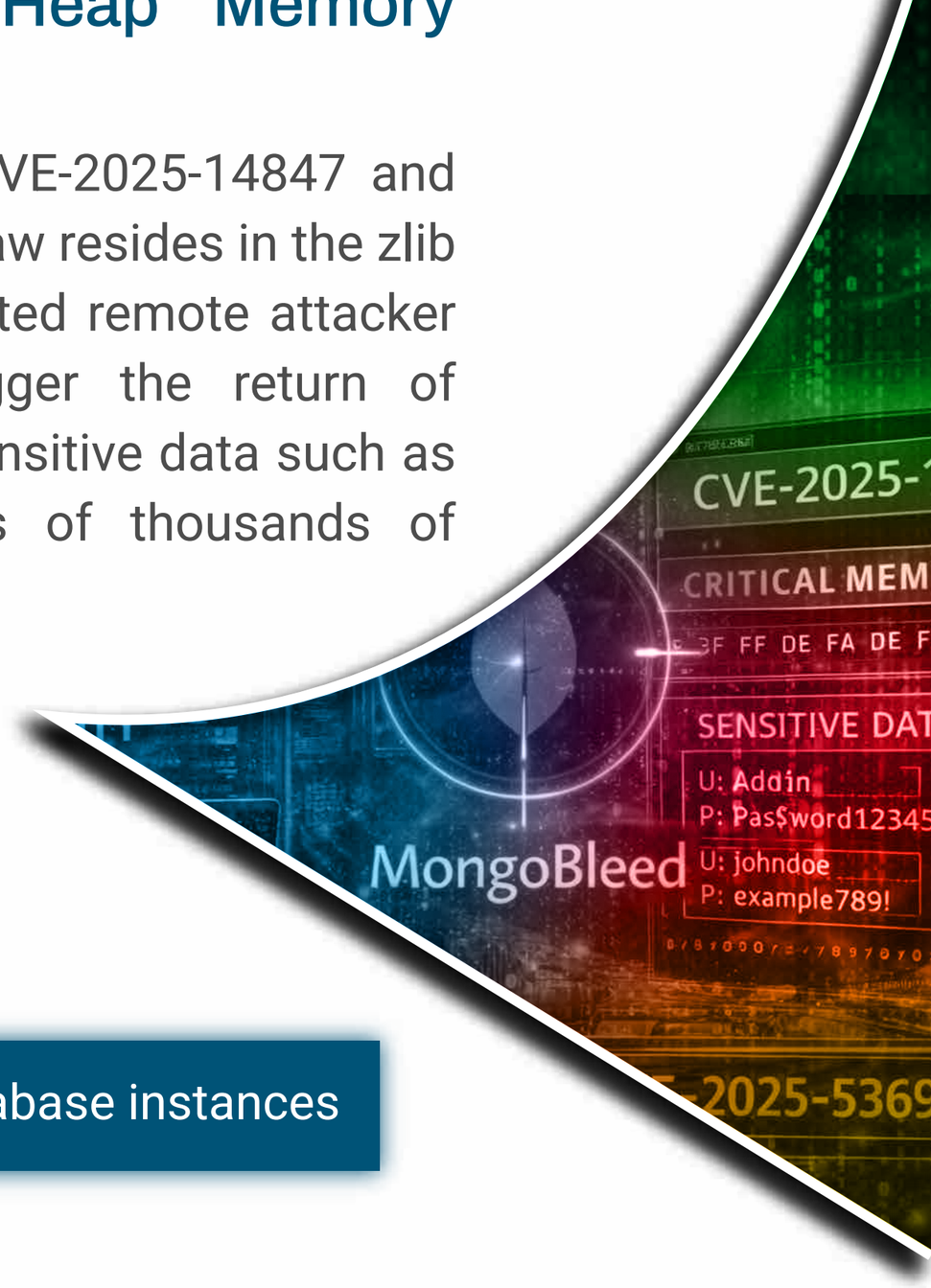
Attack Type : Zero-Day

Causes : Insecure Deserialization (Default Cryptographic Keys)

Takeaway : Rotate default machine keys and monitor for unauthorized RDP activity

MongoBleed (CVE-2025-14847): Critical Heap Memory Disclosure in MongoDB

A critical vulnerability in MongoDB Server, tracked as CVE-2025-14847 and dubbed "MongoBleed," is seeing active exploitation. The flaw resides in the zlib network message decompression logic. An unauthenticated remote attacker can send malformed compressed requests that trigger the return of uninitialized heap memory. This exposure risks leaking sensitive data such as credentials, session tokens, and API keys from tens of thousands of internet-exposed instances.



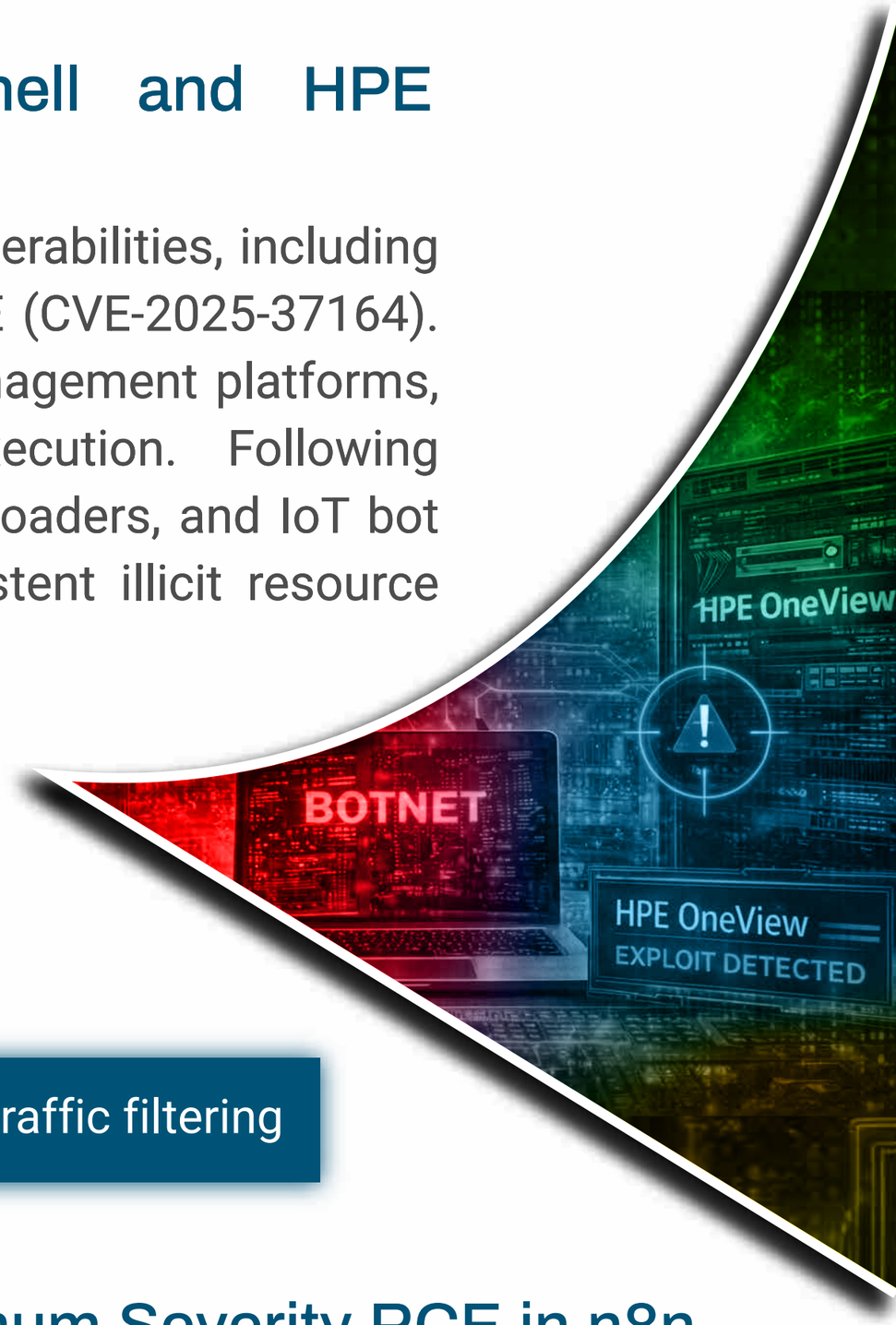
Attack Type : Memory Disclosure

Causes : Improper Decompression Logic (zlib)

Takeaway : Apply patches immediately or restrict access to database instances

RondoDox Botnet Weaponizes React2Shell and HPE OneView Flaws

The RondoDox botnet is actively weaponizing critical vulnerabilities, including React2Shell (CVE-2025-55182) and an HPE OneView RCE (CVE-2025-37164). By targeting exposed web servers and infrastructure management platforms, the botnet achieves unauthenticated command execution. Following compromise, it deploys cryptocurrency miners, malware loaders, and IoT bot clients to facilitate large-scale DDoS attacks and persistent illicit resource hijacking across global networks.



Attack Type : Botnet Recruitment

Causes : Critical Unpatched Vulnerabilities (React/HPE)

Takeaway : Patch Next.js/HPE OneView and implement egress traffic filtering

Ni8mare (CVE-2026-21877): Maximum Severity RCE in n8n Platform

The n8n workflow automation platform has disclosed a CVSS 10.0 RCE vulnerability, tracked as CVE-2026-21877. The "Ni8mare" flaw stems from the unsafe handling of workflow logic, allowing an authenticated user to execute untrusted code on both self-hosted and Cloud instances. This can result in a total system compromise, allowing attackers to hijack automated business processes, exfiltrate API secrets, and pivot into connected enterprise applications and cloud environments.

Attack Type : Remote Code Execution (RCE)

Causes : Unsafe Code Execution Logic

Takeaway : Upgrade n8n to latest patched versions to secure automation flows

Trend Micro Apex Central RCE (CVE-2025-69258) Exploitation

Trend Micro has issued an urgent advisory for a critical remote code execution vulnerability in the Apex Central management platform (CVE-2025-69258). An unauthenticated attacker can exploit an input validation flaw to execute arbitrary commands on the server. Active exploitation has been confirmed, potentially leading to full administrative takeover of the security management console, which governs endpoint protection policies across the entire corporate network.

Attack Type : Remote Code Execution (RCE)

Causes : Input Validation Flaw

Takeaway : Restrict console access and apply security patches immediately

Telnetd Authentication Bypass (CVE-2025-6616) Targets Embedded Devices

Security researchers report mass exploitation of a critical vulnerability in the telnetd daemon found in numerous embedded devices and networking hardware (CVE-2025-6616). The flaw allows remote, unauthenticated attackers to execute commands with root privileges by bypassing standard authentication checks. Compromised devices are frequently integrated into massive botnets, used as pivot points for internal network attacks, or utilized for large-scale DDoS campaigns.

Attack Type : Remote Code Execution (RCE)

Causes : Unsecured Telnet Service Logic

Takeaway : Disable Telnet and transition to SSH for all device management

Microsoft Office Zero-Day (CVE-2026-21509) Document Exploitation

Microsoft has confirmed the active exploitation of a zero-day vulnerability in Office, tracked as CVE-2026-21509. The flaw is triggered by malformed documents, enabling attackers to execute arbitrary code without direct user interaction beyond opening the file. This vulnerability bypasses standard sandboxing protections, allowing adversaries to deliver secondary payloads such as ransomware or spyware directly to the memory of enterprise workstations running vulnerable builds.

Attack Type : Zero-Day

Causes : Malformed Document Parsing

Takeaway : Enable Protected View and restrict macro-enabled documents via GPO

Malware, RATs & Botnets

Silver Fox Targets Indian Taxpayers with Modular ValleyRAT

China-linked threat actor Silver Fox is targeting Indian users with income-tax themed phishing emails delivering the modular ValleyRAT. The campaign uses malicious ZIP files and installer packages that leverage DLL hijacking to deploy the payload. Once established, ValleyRAT ensures persistence and enables comprehensive credential theft, environmental surveillance, and remote system control, utilizing SEO poisoning to drive victims toward malicious download portals.

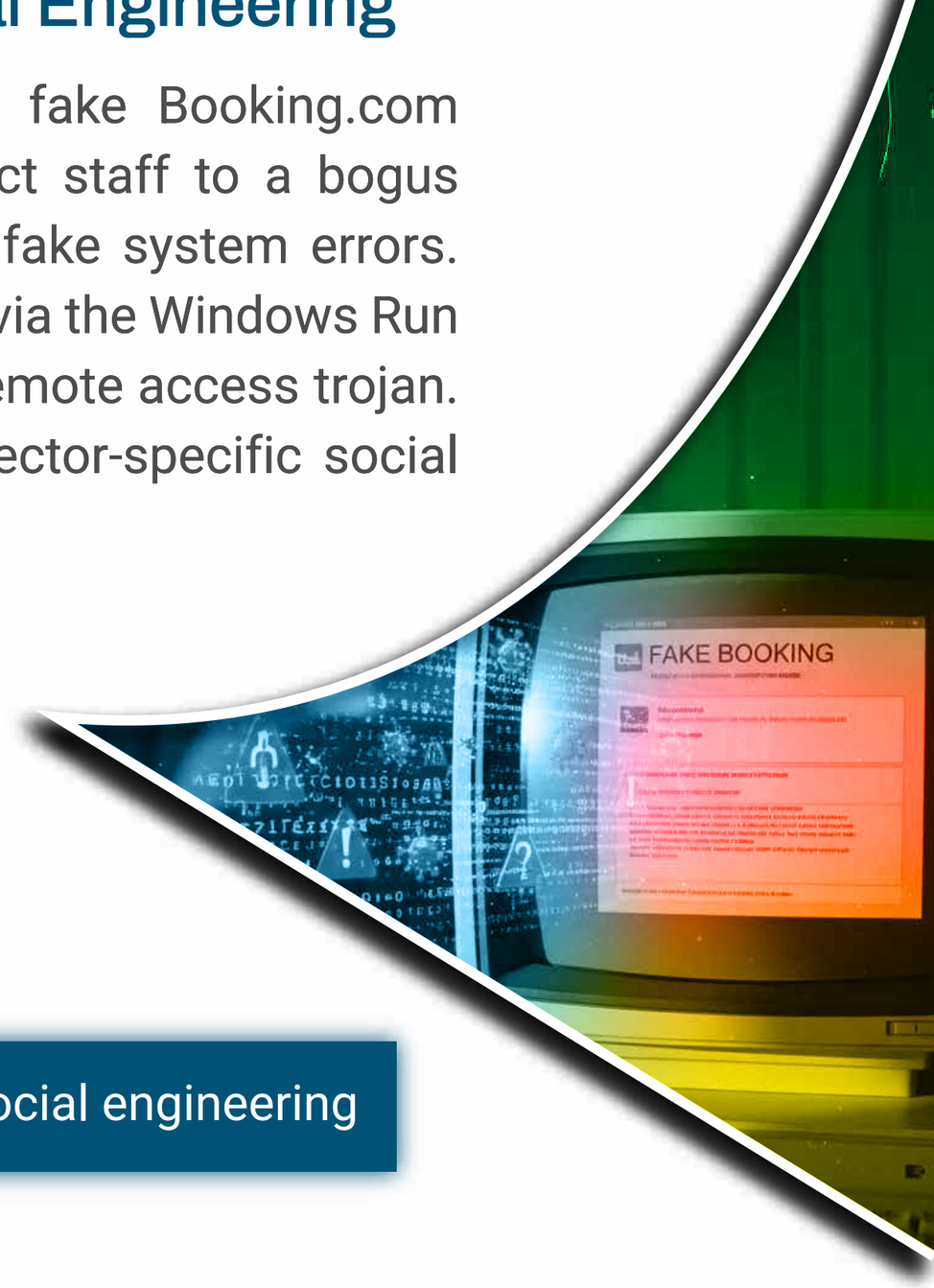
Attack Type : Phishing

Causes : DLL Hijacking and Social Engineering

Takeaway : Implement software execution controls and monitor tax-themed links

Fake Booking Emails Deploy DCRat via Social Engineering

Threat actors are targeting the hospitality sector with fake Booking.com reservation cancellation emails. These messages redirect staff to a bogus portal that mimics the legitimate platform and displays fake system errors. Victims are tricked into executing a PowerShell command via the Windows Run dialog to "fix" the issue, which silently installs the DCRat remote access trojan. This multi-stage attack highlights the effectiveness of sector-specific social engineering.



Attack Type : Phishing

Causes : Execution of Malicious Shell Commands

Takeaway : Restrict "Run" command access and train staff on social engineering

VVS Stealer: Information Theft Targeting Discord and Crypto

A new malware strain named VVS Stealer is spreading through Discord channels disguised as legitimate links or attachments. Once executed, it specifically targets stored credentials, authentication tokens, and browser data related to Discord accounts and cryptocurrency wallets. The malware exfiltrates sensitive information to attacker-controlled servers, facilitating account hijacking and financial theft within communities that rely on Discord for crypto transactions.

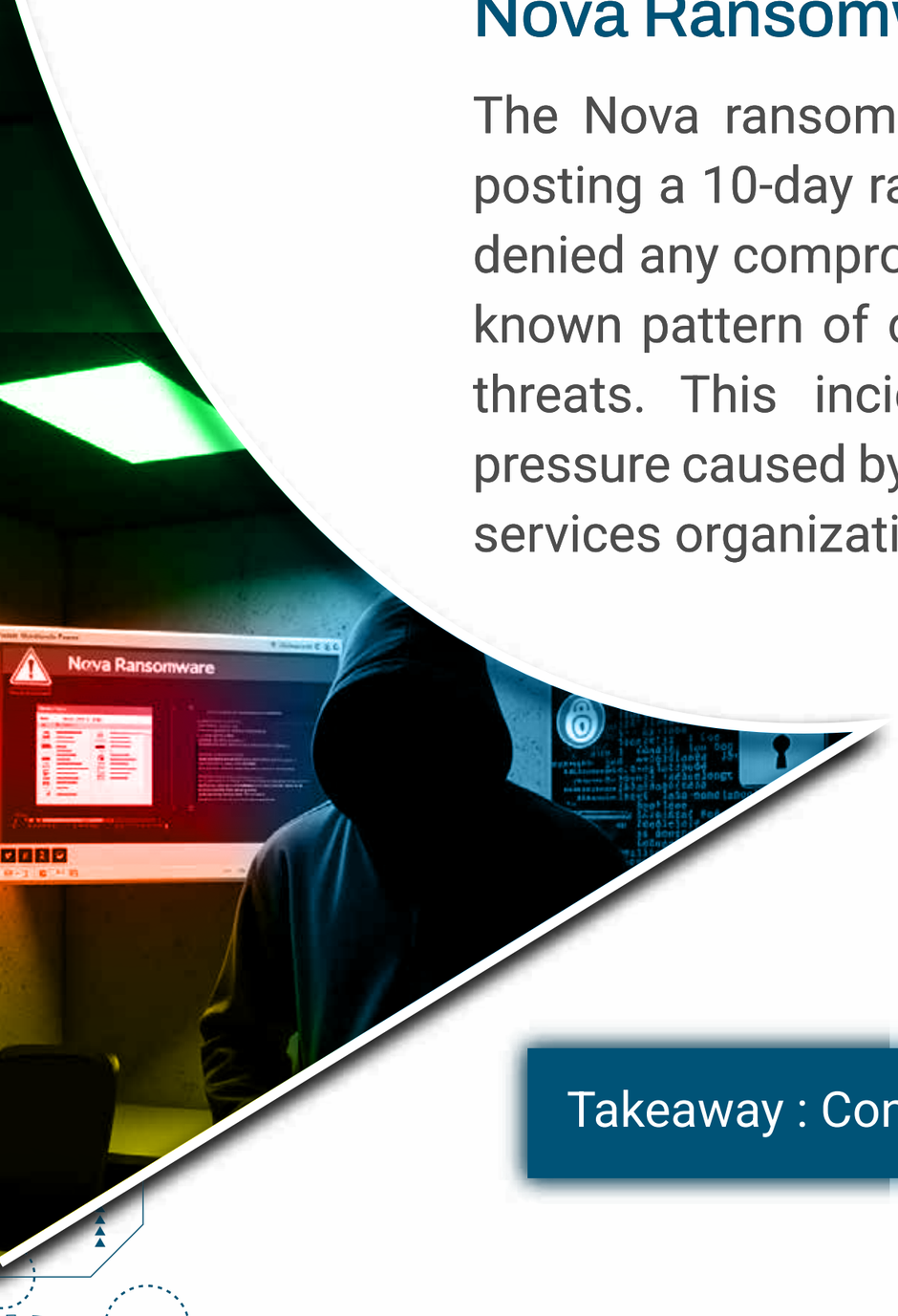
Attack Type : Information Stealer

Causes : Execution of Malicious Discord Attachments

Takeaway : Use hardware-based MFA and avoid clicking unverified Discord links

Nova Ransomware Claims Breach of KPMG Netherlands

The Nova ransomware group has claimed a breach of KPMG Netherlands, posting a 10-day ransom ultimatum on its leak site. While KPMG has officially denied any compromise of its managed systems, the claim follows the group's known pattern of double-extortion tactics involving data theft and encryption threats. This incident emphasizes the reputational risk and operational pressure caused by high-profile ransomware claims against global professional services organizations.



Attack Type : Ransomware

Causes : Potential Credential Compromise or Exploitation

Takeaway : Conduct thorough impact assessments and maintain robust IR plans

NodeCordRAT: Supply Chain Threat via Malicious npm Packages

Security researchers discovered malicious npm packages masquerading as Bitcoin libraries that deliver the NodeCordRAT. Upon installation by developers, post-install scripts deploy the payload, which steals browser credentials, API tokens, and cryptocurrency wallet data. Using Discord for command and control (C2), the malware highlights the growing risks in open-source supply chains and the critical need for verifying third-party developer tools and dependencies.

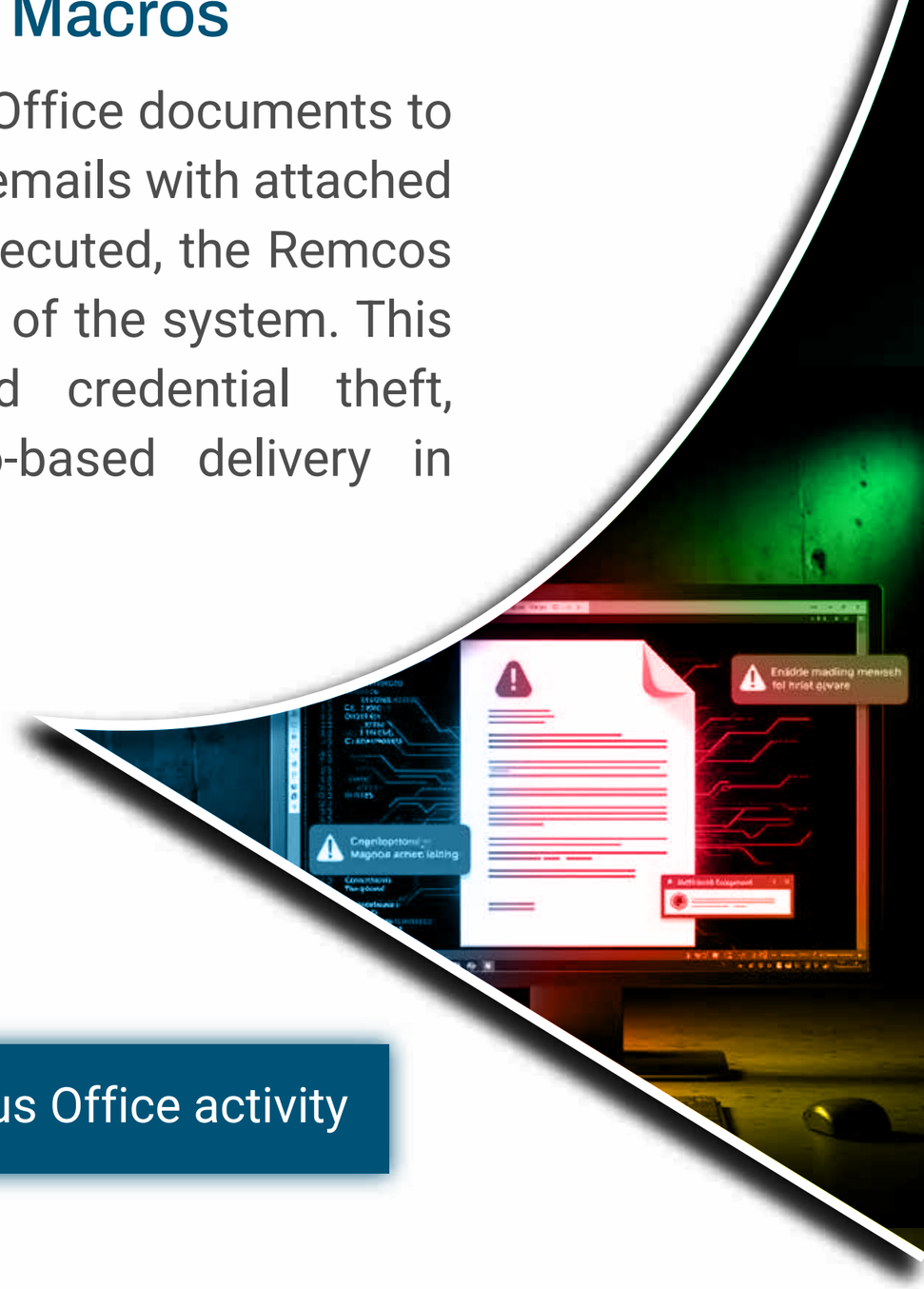
Attack Type : Supply Chain Malware

Causes : Malicious npm Packages and Post-Install Scripts

Takeaway : Audit npm dependencies and use tools to scan for malicious scripts

Remcos RAT Distribution via Malicious Office Macros

A new malware campaign is utilizing malicious Microsoft Office documents to deliver the Remcos remote access trojan. Victims receive emails with attached or linked files prompting them to enable macros. Once executed, the Remcos payload is downloaded, granting attackers remote control of the system. This allows for screen capture, keystroke recording, and credential theft, demonstrating the continued effectiveness of macro-based delivery in bypassing email security filters.



Attack Type : Malware

Causes : Malicious Office Macros and Social Engineering

Takeaway : Disable macros by default and monitor for anomalous Office activity

NINE YEARS OF UNYIELDING TRUST AND GLOBAL CYBERSECURITY EXCELLENCE

CREST Gold Standard for VA & PT

Authorized CERT-In Auditor

90+ Editions of Global Threats Intelligence

India book of Records
8k Vuln's in 4 hrs

BriskInfosec™
VULNERABILITY TO VICTORY

International Presence at GITEX Dubai & Europe

Global Footprint
24+ Countries, 4800+ Projects

Pioneers of the bSAFE & LURA Security Portal

Recognized by Industry Leaders TLG & CIO World

Author of Industry Book V2 Victory

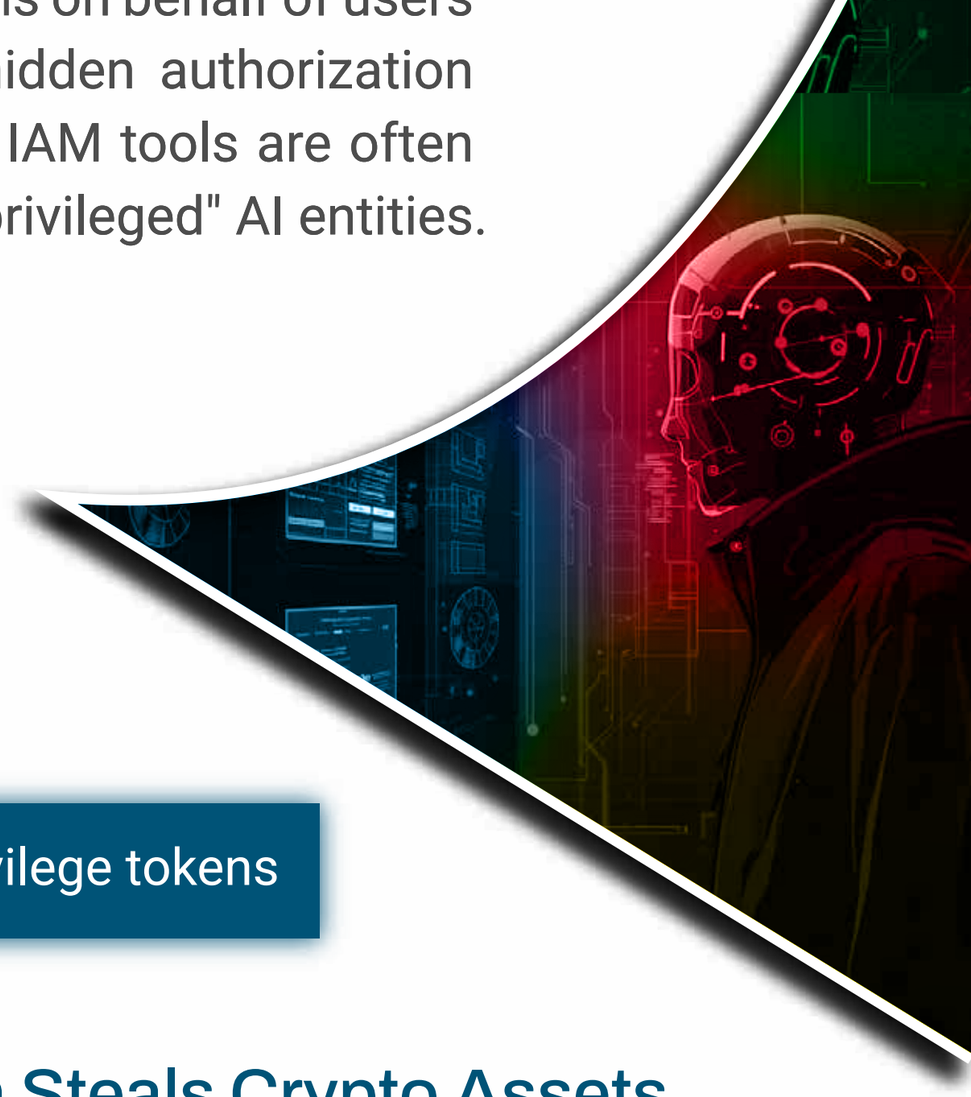
"Beyond the records and certifications, our greatest achievement is the trust you place in us every day. Thank you for nine years of shared success and an even brighter future ahead."

ARULSELVAR THOMAS
Founder & Director

Web, Browser & AI Security

Enterprise AI Agents: A New Path for Privilege Escalation

Enterprise AI agents are evolving into powerful automated identities that carry broad system permissions. Because they often operate with elevated service tokens or shared accounts, these agents can execute actions on behalf of users that exceed the user's original privileges. This creates hidden authorization bypass paths and privilege escalation risks, as traditional IAM tools are often unable to monitor the autonomous actions of these "over-privileged" AI entities.



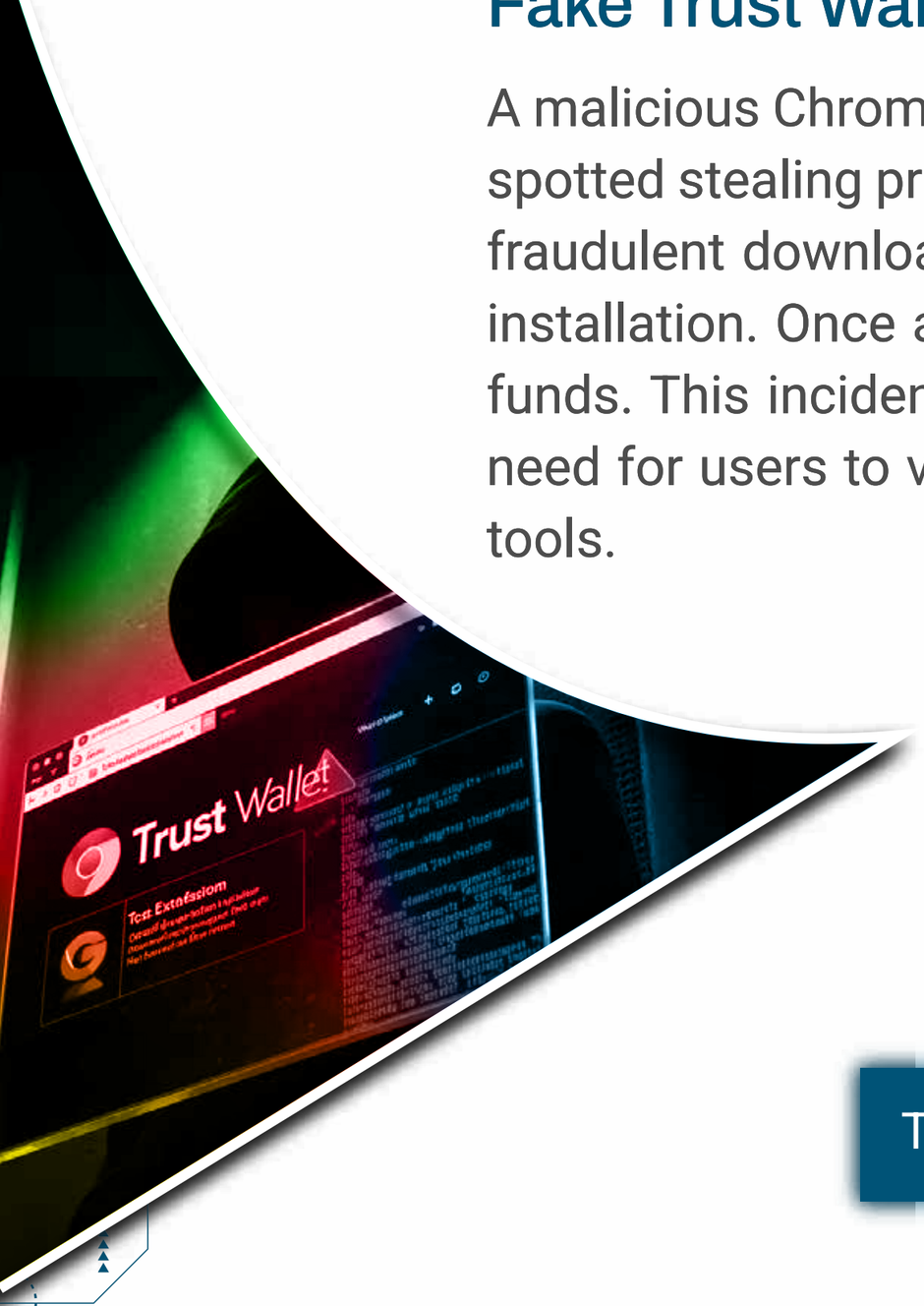
Attack Type : Privilege Escalation

Causes : Over-Privileged Autonomous Agents

Takeaway : Audit AI agent permissions and implement least-privilege tokens

Fake Trust Wallet Chrome Extension Steals Crypto Assets

A malicious Chrome extension impersonating the official Trust Wallet has been spotted stealing private keys and seed phrases. Promoted via social media and fraudulent download pages, the fake extension tricks victims into a malicious installation. Once activated, it captures sensitive wallet credentials and drains funds. This incident highlights the risk of fraudulent browser add-ons and the need for users to verify sources before installing cryptocurrency management tools.



Attack Type : Crypto Theft

Causes : Deceptive Extensions and Social Engineering

Takeaway : Only install extensions from verified, official store links

Man-in-the-Middle Chrome Extensions Steal Web Credentials

Two malicious Chrome extensions disguised as legitimate productivity tools have been caught intercepting user credentials, cookies, and API keys. Acting as man-in-the-middle proxies, the extensions injected hard-coded proxy credentials to capture traffic from over 170 popular websites. This allowed the attackers to exfiltrate session data and authentication tokens silently, underscoring the severe security implications of unvetted browser extensions in corporate environments.

Attack Type : Credential Theft

Causes : Malicious Browser Extension Proxies

Takeaway : Implement browser extension whitelisting and monitor proxy settings

Fake CAPTCHA Ecosystem Exploits User Trust to Deliver Malware

A growing wave of malware campaigns is abusing fake CAPTCHA pages that mimic trusted verification interfaces. These pages exploit user familiarity with web verification prompts to trick victims into executing commands or downloading malicious payloads. This fragmented but pervasive threat pattern leverages trusted web infrastructure to serve malware lures, effectively turning standard security verification surfaces into a primary vector for initial system compromise.

Attack Type : Malware Distribution

Causes : Deceptive Web Verification Interfaces

Takeaway : Educate users on identifying unusual verification prompts/downloads

NexShield: Fake Ad Blocker Used for ClickFix Crash Attacks

A malicious Chrome extension named NexShield, disguised as an ad blocker, is being used for "ClickFix" attacks. The extension deliberately crashes the browser to trigger a fake "repair" prompt. This social engineering tactic tricks users into running a PowerShell command that installs a backdoor for credential theft. The incident highlights the risks of unverified browser add-ons and the use of intentional system instability as a lure for malicious software execution.

Attack Type : Social Engineering

Causes : User-Triggered Shell Commands via Fake Repair Prompt

Takeaway : Restrict extension installation and block unauthorized shell commands

BriskInfosec
VULNERABILITY TO VICTORY

www.briskinfosec.com

Global Operations & Compliance

INTERPOL Operation Sentinel: Global Cybercrime Enforcement

INTERPOL's Operation Sentinel coordinated a major crackdown on cybercrime across 19 African countries, resulting in 574 arrests. The operation targeted infrastructure used for business email compromise (BEC), digital extortion, and ransomware. Law enforcement dismantled thousands of malicious links and seized devices, significantly disrupting organized online crime. This multi-nation effort strengthens regional capabilities and highlights the impact of coordinated global action.

Attack Type : Cybercrime Enforcement

Causes : Organized Global Cybercrime Activities

Takeaway : Maintain BEC protections; law enforcement is actively disrupting C2

US Treasury Lifts Sanctions on Key Intellexa Spyware Executives

The U.S. Department of the Treasury has removed sanctions from three individuals previously linked to the Intellexa Consortium, the creators of the Predator spyware. The decision followed administrative reconsideration and claims that the individuals severed ties with the organization. This move has drawn criticism from privacy advocates who argue it could weaken global accountability for the proliferation of invasive surveillance technologies used against civil society.

Attack Type : Regulatory Change

Causes : Administrative Reconsideration of Sanction Status

Takeaway : Monitor the evolving landscape of commercial spyware accountability

SHORT LESSONS IN SMARTER CYBER DEFENSE

Cybersecurity is strongest when it comes from small, practical habits in everyday digital actions, not just big tools or policies. Our awareness videos turn real risks into simple choices people can apply immediately, making security a natural part of how work gets done.

By turning incidents, new attack trends, and regulatory demands into clear lessons, this section nudges readers to fix weak habits and challenge risky defaults. These small changes steadily harden the environment and reduce the impact when attacks happen.

Watch now

BriskInfosec™
VULNERABILITY TO VICTORY

www.briskinfosec.com

“The strongest defense is not a thicker shield, but a faster understanding of the adversary’s intent.”

BriskInfosec

VULNERABILITY TO VICTORY

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