THREATSPLOIT

ADVERSARY REPORT

92nd Edition
April 2026

BriskInfosec™
VULNERABILITY TO VICTORY

www.briskinfosec.com

Dear Reader,

The boundary between a secure network and a compromised one has effectively vanished. Adversaries are no longer trying to force their way past your defenses. Instead, they are becoming a quiet part of your daily operations. This shift from brute force to deep integration within your trusted workflows marks a fundamental change in how modern threats function.

Many organizations still operate under the assumption that a strong perimeter or basic identity checks are sufficient to stop an intrusion. The reality is that your own management tools and routine processes are now the primary vehicles for sophisticated attacks. This month shows a sharp rise in the exploitation of edge infrastructure and the weaponization of identity to move silently through enterprise systems.

When an attacker hides inside a legitimate process, the risk is no longer just a technical glitch. It becomes a direct threat to your business continuity and the trust your customers place in your brand. A single overlooked misconfiguration or a compromised service account can lead to total operational paralysis before a single alert is triggered.

The April 2026 Threatsploit Adversary Report provides the clarity needed to see through the fog of thousands of daily alerts. We focus on the logic behind these movements to help you move from a reactive state to a position of true resilience. Use these insights to identify the patterns that matter and protect the core of your business.

- Briskinfosec Threat Intelligence Team

Software Supply Chain & Developer Ecosystems

1. Malicious StripeAPI NuGet Package Targets Developer Environments

Researchers have identified a malicious NuGet package masquerading as the legitimate Stripe API library to target software developers. Once integrated into a project, the package exfiltrates sensitive credentials, API keys, and environment variables to attacker-controlled infrastructure. This campaign exploits the inherent trust in open-source ecosystems and utilizes typosquatting to deceive users. It underscores the critical risks associated with automated supply chain attacks within widely used package managers.

Attack Type : Supply chain

Cause of Issue : Malicious package

Takeaway : Verify package publishers to prevent critical supply chain leaks.

2. Next.js Repository Job Scams Compromise Developer Assets

A sophisticated campaign is targeting developers via malicious repositories disguised as legitimate Next.js projects and coding assignments. Victims are lured through fake job opportunities and instructed to run code that triggers hidden execution paths. These repositories run attacker-controlled JavaScript in memory to establish command-and-control connections. By abusing Visual Studio Code workspace automation, attackers successfully steal environment variables, credentials, and sensitive internal assets.

Attack Type : Supply chain

Cause of Issue : Social engineering

Takeaway : Avoid running untrusted code for any unverified job assignments.

3. North Korean State Actors Deploy Malicious npm Package Campaign

North Korea-linked threat actors have published 26 malicious npm packages as part of a strategic supply chain operation. The packages use heavy obfuscation and hidden scripts to execute payloads that establish command-and-control via public services like Pastebin. This campaign targets developers to deploy cross-platform remote access trojans and steal crypto assets or sensitive data. It builds on previous "Contagious Interview" tactics, exploiting trust in open-source workflows to maintain persistent access.

Attack Type : Supply chain

Cause of Issue : Malicious package

Takeaway : Scan npm dependencies for obfuscation and hidden malicious payloads.

4. Malicious Go Crypto Module Deploys Linux Backdoors

Researchers uncovered a malicious Go module impersonating the legitimate golang.org/x/crypto library, designed to steal terminal passwords and deploy malware. The package injects code into password handling functions to capture sensitive inputs for exfiltration. It subsequently installs the Rekoobe Linux backdoor, enabling remote command execution and weakening firewall rules. This attack leverages namespace confusion and dependency trust to compromise developer environments and persistent server infrastructure.

Attack Type : Supply chain

Cause of Issue : Namespace confusion

Takeaway : Use checksums to verify the integrity of all Go crypto modules.

5. Self-Propagating JavaScript Worm Targets Wikipedia Integrity

The Wikimedia Foundation recently addressed a security incident involving a self-propagating JavaScript worm that vandalized thousands of Meta Wiki pages. Originating from a malicious script on Russian Wikipedia, the worm spread by injecting code into user and global JavaScript files. Within minutes, it impacted dozens of accounts and altered nearly 4,000 pages, forcing engineers to disable editing temporarily. The attack highlights risks associated with script execution and the speed at which automated worms can disrupt media platforms.

Attack Type : Worm

Cause of Issue : Script execution

Takeaway : Monitor and audit third-party user scripts on all public wikis.

6. Fake Claude Code Guides Distribute Amatera Infostealer

Threat actors are utilizing "InstallFix" attacks to distribute infostealer malware through fraudulent installation guides for developer tools like Claude Code. Malicious pages mimic official documentation to trick users into executing tampered terminal commands. These commands fetch payloads that deliver the Amatera Stealer, designed to exfiltrate credentials, session tokens, and crypto wallet data. The attack exploits developer trust in copy-paste workflows and the use of legitimate-looking domains to bypass traditional security.

Attack Type : Infostealer

Cause of Issue : Malicious instructions

Takeaway : Never copy-paste terminal commands from unofficial guides.

ACHIEVERS SPOTLIGHT

MERVIN

“ With strong commitment and the certification opportunity arranged by Briskinfosec, I was able to achieve this milestone. Their continuous guidance, support, and learning resources made this journey successful and rewarding.

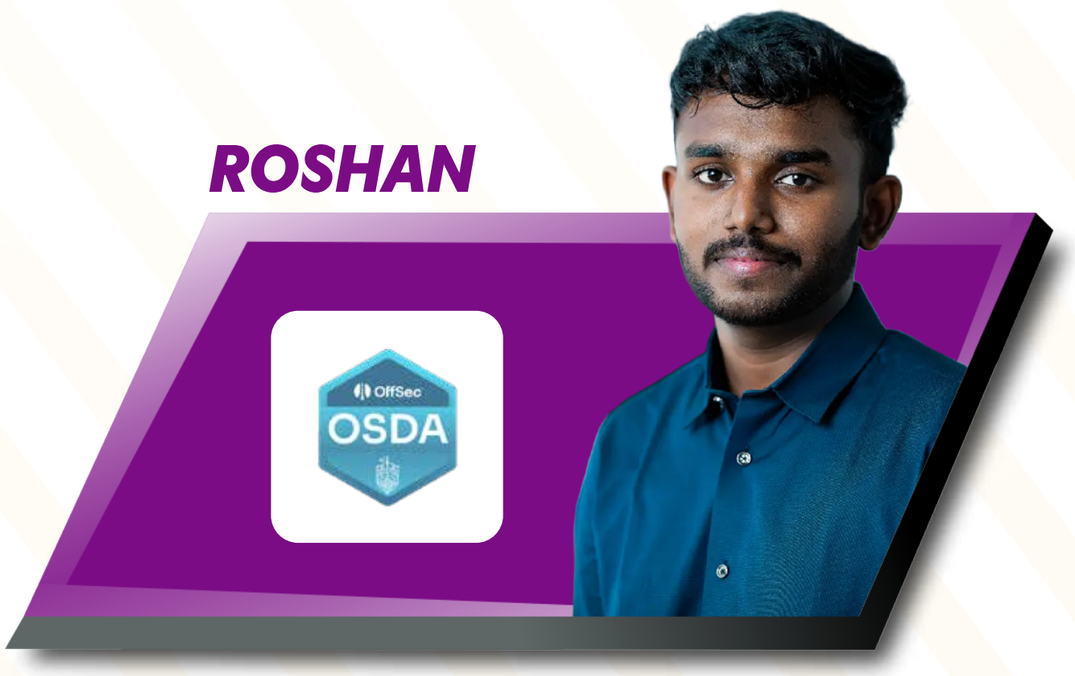
SEVUGAPERUMAL

“ I sincerely thank Briskinfosec for the opportunity and support for OSCP+. This milestone was achieved through 82 sleepless nights of continuous learning and effort.

BABIN

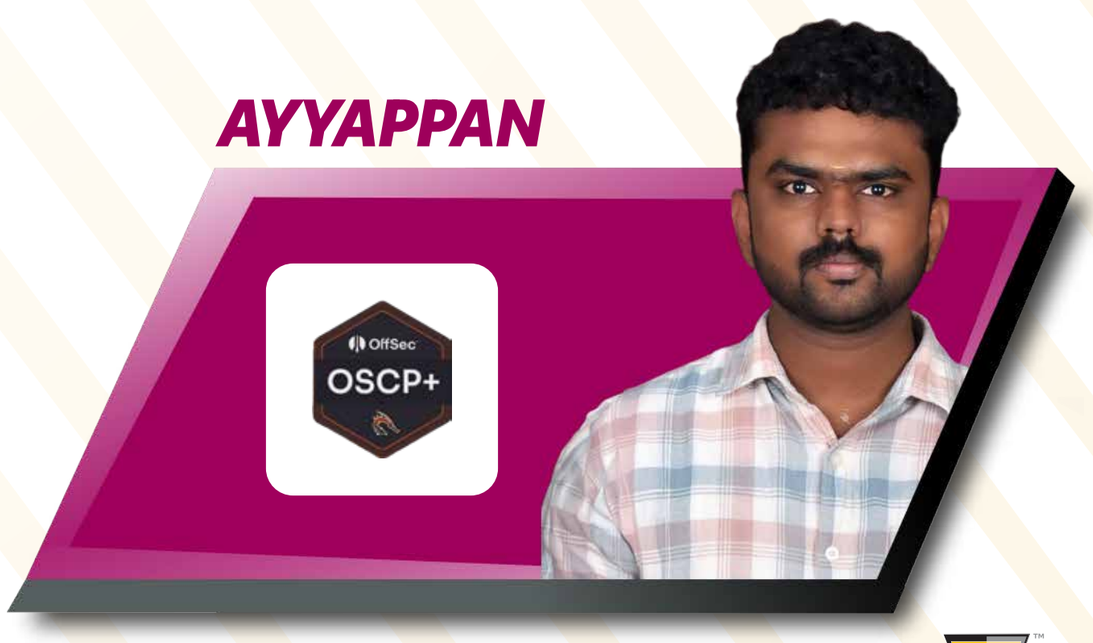
“ Earning my OSDA certification was a rewarding experience, made possible by consistent learning and real-world practice. Grateful to Briskinfosec for the opportunity, guidance, and continuous encouragement throughout this journey.

ROSHAN



“ Earning the OSDA certification marks an important milestone in my cybersecurity journey, reflecting my commitment to continuous learning and strengthening my technical expertise in offensive security and threat analysis.

AYYAPPAN



“ Earning OSCP+ wasn't easy it was a journey of trial, error and relentless learning. I’m incredibly grateful to Briskinfosec for the opportunity and to my teammates for the support that helped me stay focused and cross the finish line.

Enterprise Infrastructure & Cloud Vulnerabilities

7. Cisco SD-WAN Zero-Day Exploited for Administrative Access

A critical Cisco SD-WAN zero-day (CVE-2026-20127) has been actively exploited since 2023, allowing attackers to bypass authentication and gain administrative control. This vulnerability highlights a shift toward targeting enterprise infrastructure and cloud services for persistence. Attackers leverage weak access controls and trusted workflows to maintain a foothold in high-value environments. The report stresses that enterprise network edge devices are increasingly targeted due to their position as gateway controllers for corporate traffic.

Attack Type : Zero day

Cause of Issue : Authentication bypass

Takeaway : Patch enterprise network controllers to block unauthorized access.

8. CISA Orders Urgent Remediation of n8n RCE Vulnerability

CISA has added a critical n8n vulnerability (CVE-2025-68613) to its Known Exploited Vulnerabilities catalog following confirmed active exploitation. This flaw allows attackers to execute arbitrary code by exploiting improper handling of dynamically managed code resources within workflow executions. It poses a near-maximum severity risk to automated environments that handle sensitive credentials and integrations. Federal agencies must adhere to strict remediation deadlines to prevent unauthorized access to these high-stakes automation systems.

Attack Type : Remote code execution

Cause of Issue : Code injection

Takeaway : Patch automation tools immediately to prevent remote code injection.

9. Google Report Highlights Rise in Enterprise Zero-Day Exploits

Google's Threat Intelligence Group reported 90 zero-day vulnerabilities actively exploited in 2025, marking a significant rise in sophisticated attacks. The majority of these flaws targeted operating systems, enterprise software, and network edge devices like VPNs. Memory corruption remains the most prevalent vulnerability type across high-value infrastructure. While browser attacks have declined, exploitation of enterprise systems increased, reflecting a shift toward targets with deeper network access and higher value.

Attack Type : Zero day

Cause of Issue : Memory corruption

Takeaway : Focus security on network edge devices and enterprise systems.

10. ThreatsDay Bulletin Highlights Redis RCE and Bot Activity

The latest ThreatsDay Bulletin identifies emerging risks, including a high-severity Redis remote code execution flaw that allows arbitrary code execution on exposed systems. The report also details large-scale bot activity targeting DDR5 memory inventories and the growing use of Telegram for cybercrime automation. As malware-as-a-service platforms expand, the industrialization of cybercrime is becoming more evident through scalable infrastructure. These trends show that attackers are prioritizing automation to exploit vulnerabilities at scale.

Attack Type : Remote code execution

Cause of Issue : Buffer overflow

Takeaway : Secure exposed Redis instances to prevent arbitrary code execution.

11. FortiGate Devices Exploited to Breach Enterprise Networks

Threat actors are exploiting FortiGate devices as initial access points to breach enterprise networks and steal LDAP service account credentials. The campaign involves abusing vulnerabilities or weak credentials to extract configuration files containing sensitive network topology data. Attackers act as initial access brokers, facilitating lateral movement and subsequent malware deployment within Active Directory environments. This activity primarily targets healthcare and government sectors, highlighting the security risks of network edge devices.

Attack Type : Credential theft

Cause of Issue : Weak credentials

Takeaway : Secure edge device configurations to protect LDAP credentials.

12. Threat Actors Mass Scan Salesforce for Exposed CRM Data

Threat actors are conducting large-scale scanning of Salesforce Experience Cloud instances to extract exposed CRM data. The activity targets misconfigured portals by probing the Aura API endpoint to enumerate sensitive records without authentication. Unlike traditional exploits, this campaign abuses overly permissive guest user settings to harvest data for later phishing and vishing attacks. This activity highlights systemic risks in SaaS misconfigurations rather than specific platform vulnerabilities that require patching.

Attack Type : Data harvesting

Cause of Issue : Misconfiguration

Takeaway : Review Salesforce guest user settings to prevent massive data leaks.

13. Google Merkle Tree Certificates Aim for Quantum Resilience

Google is developing Merkle Tree Certificates (MTCs) to ensure HTTPS remains resilient against future threats posed by quantum computing. This model replaces full certificate chains with compact proofs of inclusion, reducing TLS handshake sizes and improving overall performance. A single authority can sign a tree head representing millions of certificates, allowing for scalable and efficient validation. Testing is currently underway in Chrome, with a phased rollout planned to establish a quantum-resistant root store by 2027.

Attack Type : Cryptographic risk

Cause of Issue : Quantum threat

Takeaway : Prepare infrastructure for quantum-resistant HTTPS standards.

14. Weekly Recap Highlights Qualcomm Zero-Day and iOS Exploits

A weekly cybersecurity recap highlights the active exploitation of a critical Qualcomm zero-day and a sophisticated 23-stage iOS exploit chain. These attacks represent a growing trend of multi-stage exploitation and supply chain abuse targeting mobile devices. Additionally, threat actors are leveraging Microsoft Teams for social engineering and utilizing new malware loaders for remote access trojans. The complexity of these attacks reflects an increased focus on infrastructure targets and weaknesses in existing Wi-Fi isolation mechanisms.

Attack Type : Zero day

Cause of Issue : Memory corruption

Takeaway : Implement multi-layered defenses for mobile and IoT devices.

Global APT & Nation-State Espionage

15. Silver Dragon APT Targets Governments via Cloud C2 Channels

Researchers have identified a cyber espionage campaign by Silver Dragon, an APT group linked to China, targeting government entities in Europe and Southeast Asia. Attackers gain initial access by exploiting public-facing servers and deploying multi-stage infection chains. The group uses advanced techniques such as DNS tunneling and AppDomain hijacking to maintain stealth. Notably, their GearDoor backdoor utilizes Google Drive as a command-and-control channel, allowing them to exfiltrate data through trusted cloud services.

Attack Type : APT espionage

Cause of Issue : Phishing exploitation

Takeaway : Monitor cloud service traffic for any hidden C2 communication.

16. APT28 Deploys Modified Covenant Framework for Surveillance

The Russia-linked APT28 group is utilizing a heavily modified version of the open-source Covenant post-exploitation framework in targeted espionage campaigns. The malware is deployed alongside custom implants like BeardShell to maintain persistence and capture sensitive keystrokes. By exploiting a Microsoft Office vulnerability (CVE-2026-21509) via malicious documents, the group conducts long-term surveillance of government targets. These operations demonstrate a high level of technical sophistication by blending open-source tools with custom stealth implants.

Attack Type : APT espionage

Cause of Issue : Malicious documents

Takeaway : Update Office software to patch CVE-2026-21509 vulnerabilities.

17. MuddyWater Deploys Dindoors Backdoor in Espionage Campaign

Iran-linked threat group MuddyWater has launched a cyber espionage campaign targeting banks, airports, and non-profits in the U.S. and allied regions. The attackers deployed a new backdoor named Dindoor, built on the Deno runtime, to facilitate persistent network access. The campaign involves data exfiltration through cloud storage services and reflects a focus on long-term intelligence gathering. Activity has intensified amid geopolitical tensions, demonstrating the group's commitment to infiltrating and maintaining access to high-value networks.

Attack Type : APT espionage

Cause of Issue : Initial access

Takeaway : Use network monitoring to detect any new Deno-based backdoors.

18. SloppyLemming Targets Government Sectors with Dual Malware

The threat actor SloppyLemming has launched a cyber espionage campaign targeting critical infrastructure and government sectors in Pakistan and Bangladesh. The operation utilizes distinct infection chains to deliver the BurrowShell backdoor and a specialized Rust-based keylogger. Access is gained through phishing emails containing malicious PDF lures that trigger DLL sideloading and shellcode execution. This campaign reflects an evolution in adversary tooling, using multi-stage delivery mechanisms to maintain long-term stealth.

Attack Type : APT espionage

Cause of Issue : Phishing delivery

Takeaway : Implement DLL sideloading protections against all APT actors.

INTRODUCING | Offline AI-Powered Static Application Security Testing

lurainsight

Offline SAST for Enterprise

YOUR CODE. YOUR NETWORK. YOUR CONTROL

AI-POWERED SCANNING	100% OFFLINE	PDF & XLS REPORTS	FULL DASHBOARD
Language-agnostic AI code analysis	Zero data leaves your network	Audit-ready export formats	Trends, severity, remediation

PART OF THE BRISKINFOSEC CYBERSECURITY ECOSYSTEM

LURA PORTAL | VAPT | BSOC | COMPLIANCE | LURAINSIGHT

Experience LuraInsight

BriskInfosec
VULNERABILITY TO VICTORY

www.briskinfosec.com

19. DOJ Seizes $61 Million in Tether from Pig Butchering Operations

The Department of Justice seized $61 million in Tether linked to massive "pig butchering" cryptocurrency investment scams. Victims were socially engineered through fake relationships and steered toward fraudulent trading platforms showing fabricated profits. After funds were transferred, attackers laundered the assets through multiple wallets to hide their origin. The seizure was made possible through advanced blockchain tracing and coordination with Tether, proving that law enforcement can track illicit crypto flows effectively.

Attack Type : Investment fraud

Cause of Issue : Social engineering

Takeaway : Enhanced blockchain tracing improves law enforcement recovery.

20. Phobos Ransomware Admin Faces Justice Following Extradition

A Russian national has pleaded guilty to wire fraud conspiracy for his role in administering the global Phobos ransomware operation. The group utilized a ransomware-as-a-service model, allowing affiliates to breach networks and extort over 1,000 organizations worldwide. This campaign generated tens of millions in ransom payments before the administrator was extradited from South Korea. The guilty plea marks a significant law enforcement success in disrupting the underlying infrastructure of major ransomware networks.

Attack Type : Ransomware

Cause of Issue : Credential compromise

Takeaway : Global coordination is key to dismantling ransomware networks.

21. BeatBanker Android Malware Impersonates Starlink App

A new Android malware named BeatBanker is being distributed via fraudulent websites mimicking the Google Play Store, posing as a Starlink application. Once installed, it combines banking trojan capabilities with cryptocurrency mining and the ability to tamper with transactions. Variants can deploy the BTMOB RAT, enabling full device compromise, including keylogging, screen recording, camera access, and GPS tracking. The campaign primarily targets users via sideloaded APKs and social engineering to hijack personal and financial data.

Attack Type : Mobile malware

Cause of Issue : Malicious APK

Takeaway : Avoid sideloading APKs to prevent banking trojan infections.

22. International Operation Dismantles Major LeakBase Forum

A coordinated effort by the FBI and Europol has dismantled LeakBase, a central cybercrime forum used for trading stolen credentials and hacking tools. The platform hosted over 142,000 users and hundreds of millions of compromised records before its seizure. Authorities seized databases and IP logs to further investigate key users and disrupt the wider cybercrime ecosystem. This operation involved 14 countries and approximately 100 enforcement actions, striking a major blow against data marketplaces.

Attack Type : Data marketplace

Cause of Issue : Stolen data

Takeaway : Monitoring forum takedowns provides intel on stolen user data.

Advanced Social Engineering & Botnet Operations

23. Microsoft Reveals ClickFix Campaign Abusing Windows Terminal

Microsoft has disclosed a widespread "ClickFix" social engineering campaign that tricks users into executing malicious commands via Windows Terminal. Victims are lured through fake CAPTCHA prompts and instructed to paste obfuscated commands, triggering a multi-stage infection chain. The attack eventually deploys the Lumma Stealer to exfiltrate browser credentials and sensitive system data. This evolution bypasses traditional detection by leveraging trusted system tools and legitimate workflows to compromise enterprise workstations.

Attack Type : Social engineering

Cause of Issue : User execution

Takeaway : Educate users on the risks of pasting commands into terminals.

24. Adversaries Abuse .arpa DNS to Evade Phishing Detection

Threat actors are exploiting the special-use .arpa domain and IPv6 reverse DNS to host phishing infrastructure that bypasses traditional security controls. By leveraging these infrastructure-focused records, attackers generate unusual domain formats that evade reputation checks. Since .arpa is rarely monitored for web content, phishing links can be embedded in emails without triggering standard filters. This technique showcases how core internet mechanisms are being repurposed to facilitate stealthy and effective phishing campaigns.

Attack Type : Phishing evasion

Cause of Issue : DNS abuse

Takeaway : Filter .arpa domain traffic to block infrastructure phishing.

25. KadNap Malware Compromises Edge Devices for Proxy Botnet

Researchers uncovered the KadNap malware targeting edge devices, primarily ASUS routers, to form a stealthy proxy botnet. The malware has infected over 14,000 devices by leveraging the Kademlia P2P protocol to hide its command-and-control infrastructure. This decentralized approach makes detection and takedown difficult for security teams. Compromised devices are repurposed to proxy malicious traffic, enabling threat actors to conduct brute-force attacks and further targeted exploitation while remaining anonymous.

Attack Type : Botnet

Cause of Issue : Device exploitation

Takeaway : Audit router configurations to prevent P2P botnet recruitment.

26. Aeternum Botnet Leverages Polygon Blockchain for Resilience

The Aeternum botnet utilizes the Polygon blockchain as its command-and-control infrastructure to evade traditional takedown efforts. Instead of using central servers, attackers store encrypted commands in smart contracts, which infected systems retrieve via public RPC endpoints. This decentralized approach makes the botnet highly resilient to seizure or removal by authorities. Operators can issue global instructions for delivering stealers or miners while maintaining a stealthy, persistent presence across thousands of systems.

Attack Type : Botnet C2

Cause of Issue : Decentralized infrastructure

Takeaway : Blockchain-based C2 makes botnet takedowns extremely difficult.

27. Trojanized Gaming Utilities Deliver Stealthy Java RATs

Threat actors are distributing trojanized gaming utilities via browsers and chat platforms to infect users with a Java-based remote access trojan. The attack chain uses a malicious downloader to stage a portable Java runtime and execute a disguised JAR file. By leveraging PowerShell and living-off-the-land binaries like cmstp.exe, the malware disables security protections and establishes persistence. This enables full remote control and data theft on compromised systems while evading standard detection tools.

Attack Type : Remote access

Cause of Issue : Trojanized software

Takeaway : Limit use of unverified third-party tools on work systems.

28. Microsoft Warns of OAuth Redirect Abuse in Phishing Campaigns

Microsoft has identified active phishing campaigns that exploit legitimate OAuth redirection behavior to bypass standard security filters. Attackers use manipulated redirect URIs to forward victims to malicious infrastructure after they interact with trusted identity providers like Entra ID. This technique allows for malware delivery without the need to steal OAuth tokens, making detection significantly more difficult. These campaigns primarily target government sectors, leveraging trusted authentication workflows to evade existing security controls.

Attack Type : OAuth phishing

Cause of Issue : Redirect abuse

Takeaway : Inspect redirect URIs to prevent OAuth-based phishing attacks.

29. Fake Enterprise VPN Clients Distributed via SEO Poisoning

Threat actor Storm-2561 is distributing fraudulent enterprise VPN clients masquerading as legitimate software from vendors like Cisco and Fortinet. The campaign utilizes SEO poisoning to rank malicious sites for VPN-related searches, redirecting victims to spoofed download pages. Users who install these fake clients unknowingly submit their corporate credentials to attacker-controlled servers. This attack underscores the growing abuse of search engines to facilitate credential harvesting at scale against enterprise targets.

Attack Type : Credential phishing

Cause of Issue : SEO poisoning

Takeaway : Verify VPN client downloads via official enterprise portals.

30. Global Crackdown Dismantles SocksEscort Proxy Botnet

U.S. and European law enforcement agencies have disrupted the SocksEscort proxy network, which relied on AVRecon malware to compromise edge devices. The network maintained approximately 20,000 infected devices weekly, selling residential IP access to cybercriminals for anonymous operations. Over its lifetime, it leveraged hundreds of thousands of compromised systems globally. Authorities seized domains and cryptocurrency assets, effectively disconnecting the infected devices and disrupting a major component of the cybercrime infrastructure.

Attack Type : Proxy botnet

Cause of Issue : Device compromise

Takeaway : Replace legacy edge devices to disrupt proxy botnet growth.

A NEW SPACE

A STRONGER VISION

As we continue to grow, we have officially moved into our new office space. More than just a workplace, it represents progress, ambition, and a renewed focus on building smarter solutions in an ever-evolving digital landscape. Our commitment is now even stronger as we continue to focus on delivering quality work and maintaining a robust security posture.

Bascon Futura Sv It Park, 10/2, 12th Floor, Venkatanarayana Road, T. Nagar, Chennai, Tamil Nadu 600017.

www.briskinfosec.com

Seeing clearly is the only way to stop a threat that **hides** right in front of you.

+91 44 4352 4537 | +91 73059 79769

contact@briskinfosec.com | www.briskinfosec.com