Briskinfosec's

Threatsploit Adversary Report

Edition -86 | October 2025

We are exhibiting @H23-C16

GITEX GLOBAL

13-17 OCT 2025
DUBAI WORLD TRADE CENTRE

Prabahar
Business Op. Specialist

Angel Praveena
GRC Analyst

Arulselvar Thomas
Founder & Director

Ajay Reid
Customer Success Lead

Siddique
Customer Success Exe.

Dear Readers,

The cyber battlefield is shifting in ways that challenge every organization. Attackers no longer just exploit technical flaws. They weaponize the very systems and trust relationships that businesses rely on daily. No industry is immune, and the cost of underestimating this evolution is higher than ever.

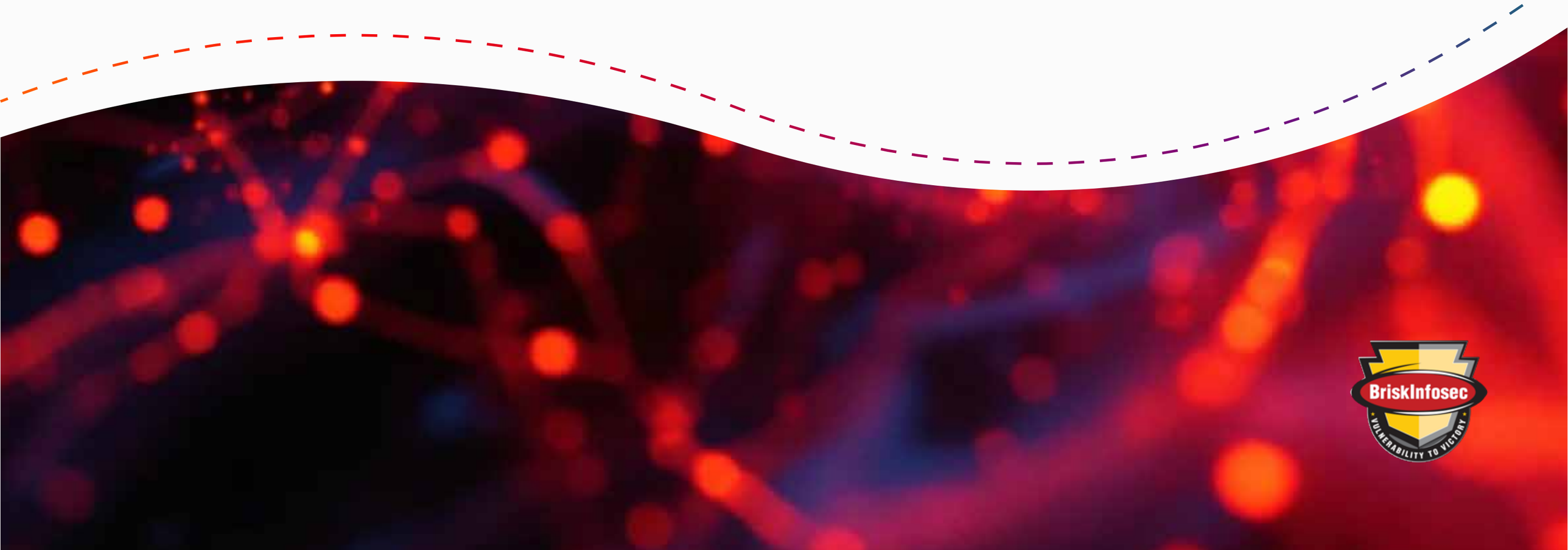
Recent Threatsploit intelligence reveals alarming trends. A leading healthcare provider exposed sensitive patient records, showing that personal data remains a prime target. In Europe, a single IT system supplier breach brought operations across 200 municipalities to a standstill, proving how supply-chain attacks can cascade far beyond the initial victim.

Innovation itself is under siege. Researchers uncovered PromptLock, the first ransomware engineered to manipulate AI prompts, signaling a new era of attacks. Meanwhile, Storm-0501 has shifted to cloud-based ransomware, exploiting weak identity controls, and organizations are discovering that Shadow IT quietly expands their attack surface.

From patient safety to public governance, AI labs to cloud environments, no sector is untouched. The path forward demands intelligence-driven security. Anticipating adversaries before they strike and treating every asset, identity, and integration as a potential entry point is critical. Reactive defense is no longer enough. The future belongs to those who can predict, prepare, and act decisively.

Best Regards,

Briskinfosec Threat Intelligence Team



Contents :

Healthcare Services Group Breach Exposes 624K Identities SSNs Financials Stolen!

Healthcare Services Group (HSGI) revealed a breach affecting 624,000 individuals, where attackers accessed and exfiltrated files with names,Social Security numbers, driver's licenses, financial details, and account credentials between September 27 and October 3, 2024, detected on October 7. The 10-month investigation concluded with notifications sent on August 25, 2025, and no evidence of data misuse found yet. The impact includes potential identity theft and financial fraud, prompting HSGI to offer 12-24 months of free credit monitoring and identity protection.

Attack Type: Data Breach | Cause: Unauthorized Access | Industry: Healthcare

Takeaways: Strengthen unauthorized access detection; provide immediate victim support like credit monitoring.

Miljödata Ransomware Cripples 200 Swedish Municipalities Ransom Demanded!

Miljödata, supplying IT systems to 80% of Sweden's municipalities, suffered a ransomware attack that disrupted services in over 200 regions, potentially stealing sensitive data and demanding 1.5 Bitcoins (~$168,000). The incident, confirmed on August 25, 2025, affected systems for medical certificates, occupational injuries, and work environment reporting, leading to operational halts. Municipalities like Halland, Gotland, and Kalmar warned residents of possible data leaks, with CERT-SE and police involved in the investigation.

Attack Type: Ransomware | Cause: Ransomware Infection | Industry: Public Sector

Takeaways: Isolate critical systems; engage authorities for rapid forensics.

PromptLock AI Ransomware Evolves Cross-Platform Encryption Steals Data!

Researchers discovered PromptLock, the first AI-powered ransomware written in Golang for Windows, macOS, and Linux, using Ollama API and gpt-oss:20b model to generate Lua scripts for file enumeration, inspection, exfiltration, and encryption with SPECK 128-bit cipher. As a proof-of-concept, it features indicators like a Satoshi Nakamoto Bitcoin wallet and unimplemented data destruction, but demonstrates AI's role in lowering attack barriers. The impact could enable novice cybercriminals to launch sophisticated, evasive attacks across platforms, complicating detection.

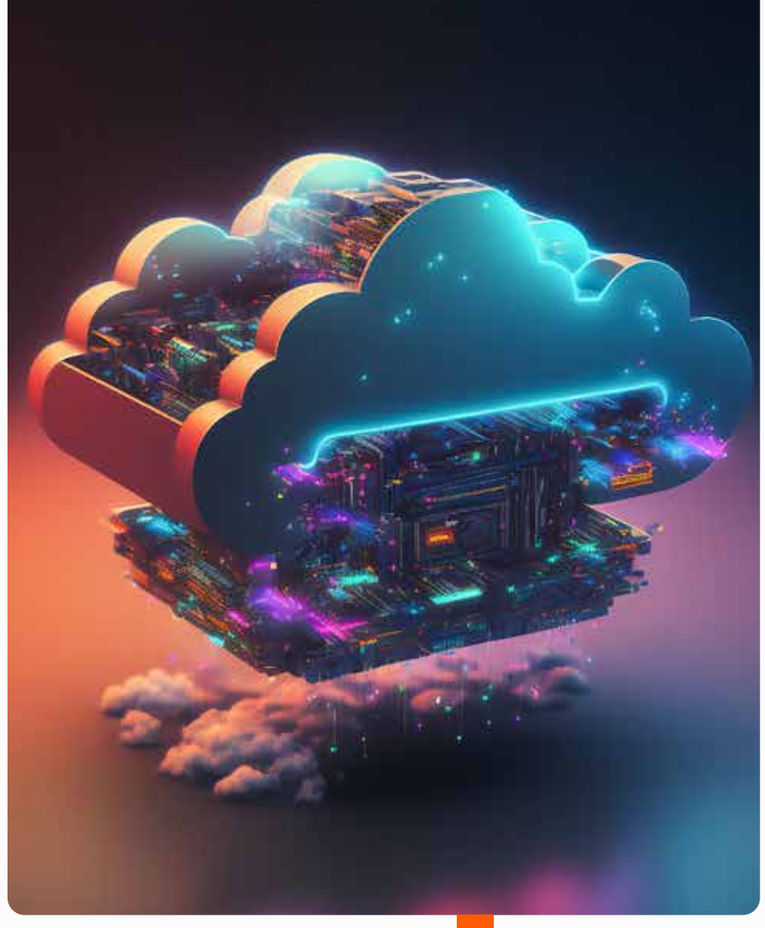
Attack Type: Ransomware

Cause: Malware Development

Industry: Information Security

Takeaways: Block AI API misuse; update EDR for script behaviors.

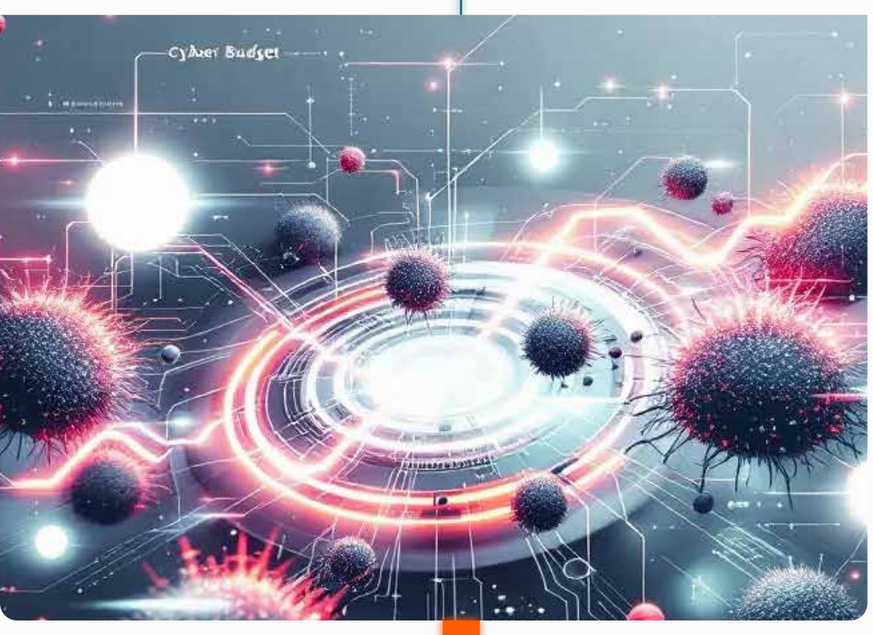
Storm-0501 Shifts to Cloud Ransomware Abuses Azure for Total Control!



Storm-0501, previously using Sabbath, Hive, BlackCat, LockBit, and Embargo, transitioned to cloud ransomware, exploiting weak Defender and MFA-lacking accounts to gain Azure control, exfiltrate data, destroy backups, and encrypt storage with new Key Vault keys. The group escalated privileges in Active Directory and Entra ID, using native tools for persistence and extortion via Microsoft Teams. This shift makes attacks stealthier, severely impacting hybrid environments with data loss and operational downtime.

Attack Type: Cloud Ransomware | Cause: Weak Identity Controls | Industry: Cloud Services

Takeaways: Enforce cloud MFA; monitor for privilege escalations.



Shadow IT Exposures Multiply Unsecured Backups Git Repos Ripe for Hack!

Intruder's research exposed shadow IT risks through subdomain enumeration and Certificate Transparency logs, uncovering unsecured backups, open Git repositories, and unauthenticated admin panels leaking credentials and sensitive data in mere days. Millions of hosts remain hidden, vulnerable to simple exploits without advanced skills. The impact amplifies attack surfaces, leading to data breaches and unauthorized access across enterprises.

Attack Type: Information Disclosure | Cause : Unmanaged Shadow IT | Industry: IT Services

Takeaways: Adopt ASM solutions; conduct regular asset inventories.

MathWorks Ransomware Hits MATLAB Devs 10K Records Pilfered!

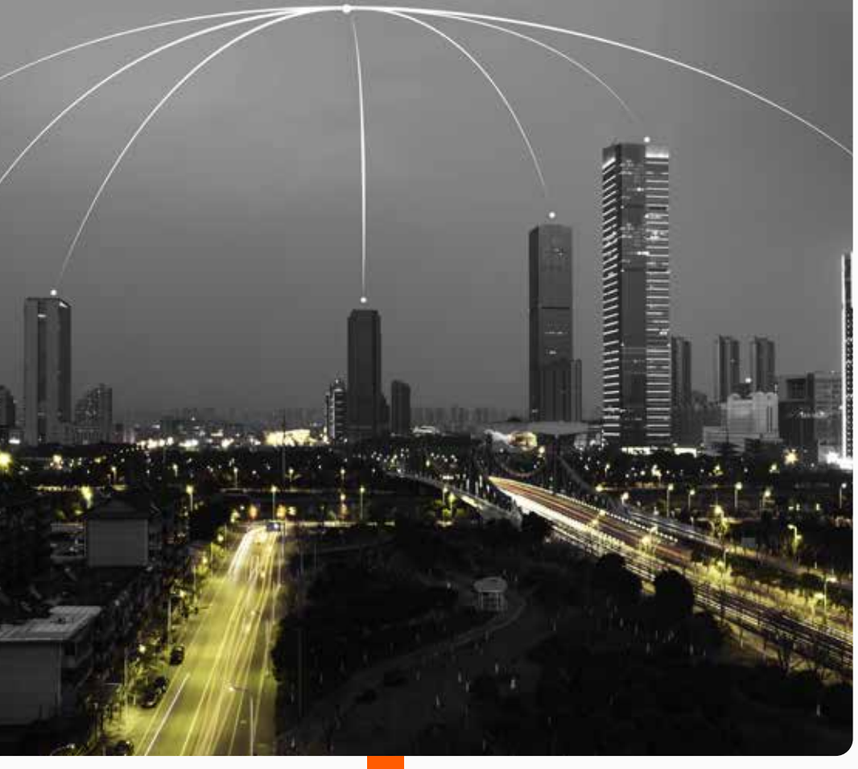
MathWorks, developers of MATLAB and Simulink, confirmed a ransomware attack compromising data of 10,476 individuals, with the breach occurring in April 2025 and discovered on May 18. Attackers accessed sensitive PII, leading to potential identity theft risks. The company notified affected parties and emphasized vigilance, though no specific method was detailed in reports.

Takeaways: Secure dev tools; implement incident disclosure timelines.

Attack Type: Data Breach

Cause: Unauthorized Access

Industry: Software Development



China-Linked PlugX Bookworm Malware Ravages Asian Telecom ASEAN Networks!

China-linked attackers deployed PlugX (Korplug/SOGU) variant with Bookworm, using DLL side-loading in legitimate apps to encrypt communications, targeting Asian telecom in ASEAN for espionage. The campaign, overlapping with RainyDay/Turian, enables persistent access and data exfiltration. Impact includes compromised network security and potential intelligence leaks in strategic sectors.

Attack Type: Malware | Cause: DLL Side-Loading | Industry: Telecommunications

Takeaways: Detect DLL anomalies; integrate APT threat intel.

COLDRIVER Malware Campaign Deploys BAITSWITCH SIMPLEFIX in Russia-Focused Hits!

Russia-linked COLDRIVER (Callisto/Star Blizzard) launched ClickFix campaigns with BAITSWITCH and SIMPLEFIX malware, using SPICA and LOSTKEYS for persistence, targeting multiple industries for espionage. The method involves lures to execute malicious code. Impact includes data theft and long-term network compromise.

Attack Type: Malware | Cause: ClickFix-Style Attacks | Industry: Multiple Industries

Takeaways: Block ClickFix lures; enhance email security.

BAS Crash Tests Prove Cyber Defenses Expose Hidden Gaps!

BAS (Breach and Attack Simulation) tools mimic adversaries to test defenses, revealing gaps like in car crash tests, essential for validating security against real threats. The method simulates attack paths to identify weaknesses. Impact helps prevent breaches by exposing unseen vulnerabilities.

Attack Type: Tooling

Cause: Simulation Gaps

Industry: Cybersecurity

Takeaways: Integrate BAS testing; prioritize simulation-based fixes.

Meet the BriskInfosec Team at

GITEX Global 2025

BriskInfosec is excited to participate in GITEX Global 2025, the world's largest technology event, where innovators, enterprise leaders, and technology enthusiasts come together to shape the future. As AI, cloud, and connected technologies continue to transform industries, we will showcase how security and innovation work hand in hand to empower organizations.

Prabahar	Angel Praveena	Arulselvar Thomas	Ajay Reid	Siddique
Business Op. Specialist	GRC Analyst	Founder & Director	Customer Success Lead	Customer Success Exe.

What You Can Explore at Our Stand :

- Personalized Cybersecurity Consultations
- Emerging Threat and Compliance Insights
- Trusted CREST-Accredited Services
- Layered Security Approach

Claim Your Free Pass

We are offering free visitor passes for this event. If you are interested in attending GITEX Global 2025, Scan the QR code and claim your pass today.

We are exhibiting @H23-C16

GITEX GLOBAL | 13-17 OCT 2025 DUBAI WORLD TRADE CENTRE

Phishing Threats Distribute CountLoader PureRAT Via Malicious SVG Files!

Phishing campaigns use malicious SVG files in emails to drop CountLoader, leading to Amatera Stealer and PureMiner through ZIP and CHM files, targeting government users for credential theft. The method tricks users into executing clipboard content, bypassing filters. Impact involves stolen data like browsers and wallets, increasing espionage risks.

Attack Type: Phishing | Cause: Deception | Industry: Government Services

Takeaways: Filter SVG attachments; educate on clipboard dangers.

Fortra GoAnywhere CVSS 10 Flaw Exploited Pre-Disclosure Command Injection Rampant!

Fortra GoAnywhere's CVE-2025-10035 command injection flaw, rated CVSS 10, was exploited as zero-day from September 10, allowing unauth RCE in MFT systems. The method involves crafted requests to execute commands. Impact includes full system compromise and data loss, with patches released in v7.8.4.

Attack Type: Exploit | Cause: Command Injection | Industry: Managed File Transfer

Takeaways: Apply patches urgently; monitor for injection attempts.

macOS XCSSET Variant Targets Firefox Clipper Persistence Modules Deployed!

Updated XCSSET malware for macOS uses encryption and obfuscation, AppleScripts for stealth, LaunchDaemon for persistence, expanding to Firefox data exfil. The method targets clipper modules for credential theft. Impact includes stolen PII and persistent infections on macOS devices.

Attack Type: Malware

Cause: Obfuscation

Industry: macOS Users

Takeaways: Deploy mac EDR; check LaunchDaemon modifications.

Cisco ASA Zero-Day Exploits Unleash RayInitiator LINE VIPER Malware!

State-sponsored actors exploited Cisco ASA zero-days to deploy RayInitiator and LINE VIPER malware, enabling backdoors in networking devices. The method involves vulnerability chaining for code execution. Impact compromises network security and data integrity in gov sectors.

Attack Type: Exploit

Cause: Zero-Day Vulnerability

Industry: Networking

Takeaways: Patch networking gear; log suspicious activity.

Cisco ASA Zero-Days Under Attack CISA Issues Emergency Directive!

Cisco patched ASA/FTD zero-days CVE-2025-20333 and CVE-2025-20362, exploited for RCE and unauth access, prompting CISA emergency directive for federal agencies. The method allows remote attacks on vulnerable devices. Impact includes potential network takeovers, with mitigations urged.

Attack Type: Exploit

Cause: Arbitrary Code Execution

Industry: Networking

Takeaways: Comply with CISA directives; isolate vulnerable devices.

Microsoft Cloudflare Seize 300 Phishing Domains RacoonO365 Dismantled!

Microsoft and Cloudflare seized 300 domains used by RacoonO365 PhaaS, exposing the leader's wallet and disrupting phishing operations. The method involved court-ordered takedown. Impact reduces phishing threats, protecting M365 users.

Attack Type: Phishing-as-a-Service

Cause: Operational Lapse

Industry: Technology

Takeaways: Pursue legal takedowns; block PhaaS domains.

FBI Warns Salesforce Users Targeted Again ShinyHunters Strike!

FBI warned of Salesforce breaches via Salesloft/Drift integrations, with ShinyHunters claiming responsibility for data theft. The method exploited third-party access. Impact exposes customer PII, prompting vigilance.

Attack Type: Hacking

Cause: CRM Exploitation

Industry: Tech

Takeaways: Audit SaaS integrations; enable advanced logging.

US Treasury Sanctions Southeast Asia Cyber Scam Networks!

OFAC sanctioned 19 entities and individuals for cyber scams using forced labor for romance and investment frauds. The method involved organized crime networks. Impact disrupts global scam operations, protecting consumers.

Attack Type: Cyber Scams | Cause: Organized Crime | Industry: Financial

Takeaways: Implement scam detection; collaborate with financial regulators.

LAPSUS$ Breaches Google LERS Exposes FBI eCheck System!

LAPSUS$ group breached Google's Law Enforcement Request System via fraudulent account, potentially exposing FBI eCheck. The method used social engineering for access. Impact risks law enforcement data exposure.

Attack Type: Hacking | Cause: Fraudulent Account | Industry: Law Enforcement

Takeaways: Verify request accounts; enhance auth for sensitive portals.

Scattered Spider Resurges Targets Banks Retail Cyber Extortion!

Scattered Spider group resurfaced, targeting banks and retail with extortion, despite claimed retirement, with members charged. The method involves sophisticated intrusion. Impact includes financial losses and data leaks.

Attack Type: Cyber Extortion | Cause: Ongoing Campaigns | Industry: Finance

Takeaways: Track group activities; develop extortion IR plans.

BreachForums Founder Resentenced 3 Years Cybercrime Facilitation!

BreachForums founder Fitzpatrick resentenced to 3 years for facilitating data and malware exchange, due to parole violation. The method involved operating dark web forum. Impact curbs cybercrime ecosystems.

Takeaways: Monitor dark web; report illegal forums.

Attack Type: Cybercrime Marketplace | Cause: Parole Violation | Industry: Technology

BriskInfosec
VULNERABILITY TO VICTORY

Find Your Organization Security Health Score

You know your balance sheet but do you know your organization's **true security status?** When high-stakes risk is on the line, multi-page technical reports don't cut it. You need a definitive answer.

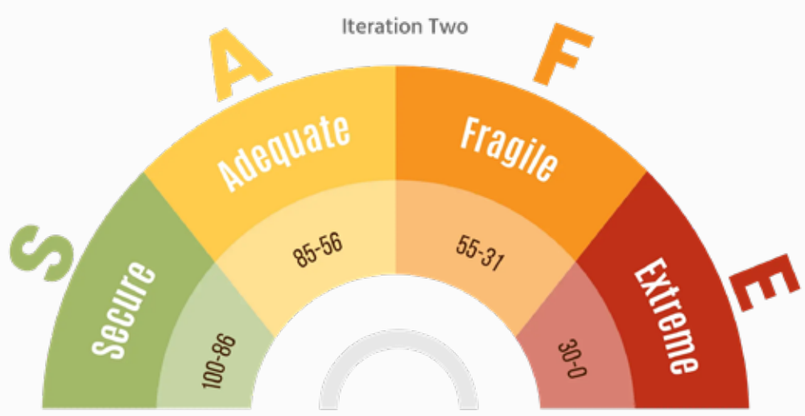
You shouldn't manage enterprise-wide cyber risk without a single, objective metric.

Briskinfosec introduces the **bSAFE Score: Your quantifiable Security Health Score.** This number moves beyond technical jargon to provide a clear, **data-driven assessment** of your entire digital defense posture. It is the immediate clarity you need to align security investments with business priorities.

The Score That Defines Your Risk: What is Your bSAFE Rating?

The **bSAFE Score** translates complex, continuous security data into a single, unambiguous number. It gives you immediate clarity on your organization's security health, moving you from technical guesswork to strategic action.Here is what your score reveals:

Score Range	Status
Secure (86-100)	Robust Posture
Adequate (56-85)	Satisfactory, but Risky
Fragile (31-55)	High Vulnerability
Extremely Vulnerable (0-30)	Severe Danger



Scan the QR code below to access information on how to get your bSAFE Score now.

Cyberattack Disrupts Check-In at Major European Airports Chaos Ensues!

A ransomware attack on Collins Aerospace disrupted check-in at European airports like Heathrow and Berlin on September 19, 2025, forcing manual operations. The method targeted aviation IT provider. Impact caused delays, cancellations, and queues for thousands.

Attack Type: Cyberattack | Cause: Ransomware | Industry: Aviation

Takeaways: Develop manual backups; test supply chain resilience.

Man Arrested for European Airports Cyberattacks Ransomware Strain Exposed!

Authorities arrested a man connected to the sophisticated ransomware attack on European airports' MUSE system, disrupting operations. The method used advanced ransomware. Impact revealed vulnerabilities in aviation tech.

Attack Type: Ransomware | Cause: Sophisticated Strain | Industry: Aviation

Takeaways: Coordinate with law enforcement; update aviation software.

Airport Disruption Cyber-Attack Hits Check-In Boarding Systems!

Cyber-attack on MUSE software by Collins Aerospace hit check-in and boarding at European airports, causing hours-long delays. The method was supply-chain attack. Impact led to manual processes and passenger chaos.

Attack Type: Cyberattack

Cause: System Targeting

Industry: Aviation

Takeaways: Enhance vendor security; conduct regular audits.

Brussels Airport Flights Cancelled Major Cyber-Attack Hits Europe!

Half of flights at Brussels Airport cancelled due to cyber-attack on European airports, affecting check-in systems. The method targeted critical infrastructure. Impact stranded passengers and disrupted travel.

Attack Type: Cyberattack | Cause: Infrastructure Hit | Industry: Aviation

Takeaways: Build cyber resilience; share incident intel.

Villager AI Framework Automates Pentests Bundles RATs Mimikatz!

Villager, AI-powered PyPI framework, automates offensive workflows with AsyncRAT and Mimikatz, spawning containers for scans from prompts, marketed for red-teaming. The method lowers misuse barriers for less-skilled actors. Impact increases rapid exploitation risks and detection challenges.

Attack Type: Tooling | Cause: Abuse | Industry: Security

Takeaways: Vet AI tools; monitor for automated attack signs.

Google Patches Chrome Zero-Day CVE-2025-10585 Memory Corruption Live!

Google patched Chrome V8 zero-day CVE-2025-10585, a type confusion for memory corruption, exploited in wild, reported by Threat Analysis Group. The method allows arbitrary code exec. Impact threatens browser users with potential compromise.

Attack Type: Exploit | Cause: : Confusion | Industry: Browser

Takeaways: Enable auto-updates; use sandboxed browsing.

New FileFix Attack Uses Steganography to Drop StealC Malware Fake Meta Alerts!

New FileFix campaign uses fake Meta suspension lures to execute clipboard PowerShell, downloading stego-images hiding scripts for StealC infostealer, exfiling creds and wallets. The method evades detection with obfuscation. Impact leads to widespread data theft and financial loss.

Takeaways: Block clipboard scripts; scan for stego content.

Attack Type: Steganography | Cause: Deception | Industry: Security

BriskInfosec

FortiSIEM RCE Exploit Loose Unauth Hackers Commandeer Security Platforms!

Fortinet warned of FortiSIEM pre-auth RCE CVE-2025-25256, exploited in wild via CLI command injection for arbitrary commands. The method allows system takeover. Impact exposes security data and enables lateral movement.

Attack Type: Remote Code Execution | Cause: Improper Sanitization | Industry: MSSP

Takeaways: Patch SIEM tools; enable input validation.

ShinyHunters Breaches Salesforce Via Drift 1.5B Records Looted!

ShinyHunters claimed breach of Salesforce via Snowflake/Drift integration, stealing 1.5B records with names, emails, and metadata. The method exploited connected platforms. Impact risks massive PII abuse and identity fraud.

Attack Type: Intrusion | Cause: Access | Industry: SaaS

Takeaways: Secure supply chains; audit connected apps.

UK Nabs Scattered Spider Teens Behind TfL Hack Healthcare Intrusions!

UK authorities arrested two teens linked to Scattered Spider for TfL hack under Computer Misuse Act, with ties to US healthcare intrusions. The method involved conspiracy for unauthorized acts. Impact disrupts transport and health services.

Attack Type: Intrusion | Cause: Conspiracy | Industry: Transport

Takeaways: Target group networks; enhance juvenile cyber education.

Top CVE's of September

CVE-2025-20333

Critical RCE in Cisco ASA/FTD VPN web server allows authenticated attackers to execute arbitrary code with root privileges via crafted HTTP requests.

Severity : Critical

Attack Type : Remote Code Execution

CVE-2025-10184

Critical SMS data leak in OnePlus OxygenOS 12–15 allows malicious apps to access and send SMS messages without user consent, impacting millions of devices.

Severity : High

Attack Type : SQL Injection

CVE-2025-10585

Critical type confusion vulnerability in Google Chrome V8 engine allows attackers to execute arbitrary code remotely, requiring immediate browser update.

Severity : Critical

Attack Type : Code Execution

CVE-2025-59814

A critical SQL injection in Zenitel ICX500/ICX510 Billing Admin allows unauthenticated attackers to access, modify, or delete sensitive billing data.

Severity : High

Attack Type : Bypass

CVE-2025-58438

A critical SQL injection in Zenitel ICX500/ICX510 Billing Admin allows unauthenticated attackers to access, modify, or delete sensitive billing data.

Severity : Critical

Attack Type : Privilege Escalation

BriskInfosec

“Security is not a product but a mindset. Anticipate, prepare, and act before the threat arrives”

BriskInfosec

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