The 2025-2026 Cyber Extortion Ecosystem - Treadstone 71

Extortion Economics and Market Fragmentation

The Treadstone 71 Ransomware Analysis

Cybercriminals shifted aggressively toward Extortion-as-a-Service (EaaS) models throughout 2025. Groups abandoned encryption entirely, focusing purely on exfiltration to minimize technical friction while maximizing reputational damage. Victims of extortion-only attacks frequently pay quietly to avoid regulatory scrutiny, resulting in untracked cryptocurrency transactions that never appear in vendor statistics. Relying on flawed telemetry produces a dangerous illusion of security, blinding organizations to the actual severity of the cybercrime ecosystem.

Record-setting numbers defined 2025, with 7,515 publicly posted ransomware victims representing a 58 percent year-over-year increase. The number of tracked ransomware groups reached an all-time high of 124, indicating a 46 percent increase from the 88 groups tracked in 2024. On average, operators posted 20.6 victims daily. Total attacks claimed rose 50 percent, making 2025 the most active year on record. The median ransom payment size increased significantly, even as the total volume of payments stagnated.

Payment rates plummeted from 63 percent in 2024 to just 29 percent. Improved incident response capabilities and increased regulatory scrutiny contributed to the decline in successful extortion attempts. Global action against ransomware operators, infrastructure, and laundering networks helped limit some revenue flows. Specific strains like VolkLocker contained cryptographic weaknesses that allowed free decryption in some cases, further reducing payouts.

Ransomware-as-a-Service (RaaS) operations experienced marked fragmentation, leading to a surge in smaller, independent groups. Initial Access Broker (IAB) activity functioned as a leading indicator for future attacks. On-chain analysis indicates that spikes in IAB inflows typically precede increases in ransomware payments and victim leaks by roughly 30 days. Criminal and state-linked actors routinely share infrastructure, complicating attribution efforts. Disruption efforts focused on the enablement layer, targeting the infrastructure supporting multiple syndicates.

Metric	2023	2024	2025
Median Ransom	$500,000	$500,000	$600,000

Metric	2023	2024	2025
Demand			
Median Ransom Payment	$150,000	$150,000	$152,750
Payment Rate	32.1%	30.2%	31.6%

Data collected during incident response engagements demonstrates consistent financial demands across major sectors. Professional, Scientific, and Technical Services remained the sector most likely to make a ransom payment, with a 37.4 percent payment rate and a median demand of $542,200. Wholesale Trade organizations faced a 28.3 percent payment rate against a median demand of $590,000. Construction firms experienced a 27.3 percent payment rate with median demands reaching $740,500. Manufacturing entities paid 25.5 percent of the time, facing median demands of $696,500. Healthcare and Social Assistance proved the most resilient, paying only 18.6 percent of the time against median demands of $500,000.

The Akira Syndicate and Perimeter Device Exploitation

Akira dominated the 2025 threat ecosystem, accounting for 28.4 percent of all observed ransomware engagements. During August 2025, the group alone was responsible for more than half of all incidents responded to by major security firms. Analysts initially attributed the massive volume to a sophisticated zero-day vulnerability. Subsequent investigations exposed a far more mundane reality driven by administrative negligence.

Attackers aggressively exploited CVE-2024-40766, an improper access control flaw within SonicWall SonicOS affecting Gen 5, Gen 6, and Gen 7 devices. Administrators applied firmware patches but routinely failed to reset local user account passwords—a mandatory remediation step explicitly detailed within the vendor's upgrade instructions. Akira operators methodically scanned the internet for specific misconfigurations, gaining unauthenticated Virtual Private Network (VPN) access to enterprise environments.

The incident exposes a severe cognitive blind spot within defensive operations: the assumption that patching equals comprehensive remediation. Threat actors retain access long after firmware updates if credentials remain compromised. Akira maintained extended dwell times, returning to environments compromised months prior to execute encryption routines and retroactively add victims to their data leak site.

Akira commanded 14.9 percent of observed engagements during the first quarter. Qilin held roughly eight percent, while Play captured approximately six percent. In the second quarter, Akira's share dropped to eight percent. Qilin doubled its presence to 16.0 percent, and Play remained stable near six percent. The third quarter witnessed an unprecedented anomaly. Akira's operations surged to capture 41.5 percent of all engagements. Qilin accounted for 12.4 percent, while Play fell to approximately four percent. During the fourth quarter, Akira maintained a dominant 33.5 percent share. Qilin rebounded to 17.7 percent, and Play stabilized around five percent.

Other ransomware syndicates, including Qilin, INC, and WhiteRabbit, adopted identical exploitation techniques throughout 2025, reinforcing SonicWall VPN vulnerabilities as a broadly weaponized entry point. The repeated exploitation of known flaws across multiple groups

highlights the scalability of perimeter device abuse. Akira's operational success stems not from advanced persistent threat tactics, but from the industrialization of opportunistic exploitation.

Akira's initial access methods reveal a methodical approach. VPN systems without multi-factor authentication represent the preferred target. The group exploits known vulnerabilities in Cisco VPN solutions alongside SonicWall. Poorly secured Remote Desktop Protocol (RDP) connections serve as another favorite attack vector, exploited via brute force techniques or compromised credentials. Akira's spear-phishing campaigns feature customized lures tailored to the specificities of each target organization.

Following an article published on Habr—a media platform focused on technology and internet culture—that revealed weaknesses in Akira's encryption, rival syndicates took notice. The DragonForce ransomware cartel quickly reinforced its own encryptor to avoid similar problems. DragonForce, a Conti-derived ransomware-as-a-service active since 2023, employs Bring Your Own Vulnerable Driver (BYOVD) attacks. The group uses truesight.sys and rentdrv2.sys drivers to terminate security processes. DragonForce rebranded as a ransomware cartel, allowing affiliates to white-label payloads and create variants like Devman and Mamona/Global.

Qilin's Ascendance and State-Sponsored Franchising

The historical demarcation between financially motivated cybercrime and state-sponsored espionage collapsed entirely in 2025. The Qilin RaaS operation scaled rapidly throughout the year, becoming the second most prolific syndicate globally. The group transitioned its codebase to the Rust programming language, enabling stealthy in-memory execution and cross-platform compatibility.
In March 2025, intelligence analysts identified Moonstone Sleet, a North Korean state-sponsored threat actor, actively deploying Qilin ransomware payloads. The Democratic People's Republic of Korea effectively franchised a Russian-speaking cybercrime toolset to generate state revenue and disrupt Western industrial infrastructure.

The partnership benefits the two entities substantially. Qilin gains a highly capable, nation-state affiliate network capable of executing complex initial access operations. Moonstone Sleet acquires sophisticated encryption tooling, robust negotiation infrastructure, and the plausible deniability afforded by operating under a known cybercriminal brand. The convergence of state actors and criminal syndicates fundamentally alters the risk calculus for enterprise defenders, as organizations face nation-state resources deployed for immediate financial extortion.
Beyond SonicWall, threat actors systematically targeted specific edge appliances and remote management tools to secure initial access. Exploitation focused heavily on Fortinet devices, specifically abusing CVE-2024-55591 within FortiManager and CVE-2025-24472 within FortiOS. Attackers employed crafted requests to bypass authentication entirely, escalating privileges to super-admin status.

Qilin functioned as the primary syndicate exploiting Fortinet vulnerabilities. The group combined Secure Sockets Layer (SSL) VPN access with exposed File Transfer Protocol (FTP) services to deploy web shells and establish deep persistence. Once administrative access materialized, threat actors dumped configuration files containing plaintext credentials, executing lateral movement into Windows environments before staging ransomware payloads.

Qilin emerged as the most active threat group starting in the second quarter of 2025, following the sudden departure of the RansomHub threat group from the ransomware ecosystem. Qilin accounted for 101 incidents in Q2, significantly increasing from 21 incidents in Q1. The group became noticeably more aggressive, averaging 75 victims per month during peak operations. Regional concentration shifts occurred, with South Korea entering the top ten list of most attacked countries following a focused campaign by Qilin targeting its financial sector.

Code Proliferation- The INC, Lynx, and Sinobi Lineage

Law enforcement disruptions in early 2024 forced a massive restructuring of the Ransomware-as-a-Service economy. The resulting vacuum accelerated codebase sharing, intellectual property theft, and rapid rebranding among syndicates. An empirical examination of the INC Ransom, Lynx, and Sinobi families reveals a shared architectural lineage that challenges traditional attribution methodologies.

In May 2024, an actor operating under the alias "salfetka" allegedly sold the source code for INC Ransom on the XSS hacking forum. Shortly thereafter, Lynx ransomware emerged in the wild. By mid-2025, the Sinobi Group surfaced, displaying overwhelming technical similarities to Lynx. Binary analysis confirms a 99 percent code similarity between Lynx and Sinobi.
The three variants employ a hybrid encryption architecture combining AES-128 symmetric algorithms and Curve25519 elliptic curve cryptography. The ransomware families share identical file encryption logic, overlapping command-line arguments, and perfectly matched metadata structures within their encrypted files. Furthermore, the underlying structure, interface components, and routing behavior of their respective data leak sites originate from the exact same source code.

Sinobi executes sophisticated defense evasion techniques derived directly from its predecessors. Before initiating encryption, the malware deletes all files residing within the Recycle Bin using the SHEmptyRecycleBinA Application Programming Interface (API). The program subsequently enumerates hidden volumes, mounting them to maximize the scope of the destructive process.
The most alarming capability involves the destruction of volume shadow copies via direct device access. Instead of executing standard command-line utilities like vssadmin—which security operations centers routinely monitor—Sinobi interacts directly with the driver using the undocumented IOCTL_VOLSNAP_SET_MAX_DIFF_AREA_SIZE control code. By setting the input buffer to zero, the malware forces the Windows operating system to resize the "diff area" storage location. The operation compels the system provider to automatically delete all existing snapshots to free up space. Detections relying solely on command-line parameter monitoring fail entirely against direct kernel-level manipulation.

The Sinobi group operates under a semi-private Ransomware-As-A-Service model, employing dual extortion to ensure payout. The group only works with known, vetted affiliates, allowing them to maintain high operational security and evade law enforcement infiltration. Sinobi witnessed a 300 percent operational surge in the fourth quarter of 2025, claiming 149 victims and becoming the third most prolific ransomware group globally.

The Interlock Syndicate and Remote Access Trojans

The Interlock ransomware group emerged in September 2024, demonstrating sophistication consistent with experienced operators. Interlock develops its own malware to facilitate attacks and does not operate as a traditional public RaaS. The group avoids advertising on dark web forums, maintaining a low profile while executing high-impact intrusions.

Interlock relies heavily on credential access purchased from initial access brokers. The group executes session hijacking with valid tokens, allowing attackers to impersonate users without knowing passwords or completing MFA challenges. Interlock operators abuse legitimate cloud utilities like AzCopy and Cloudflare tunnel services for command-and-control communications and data exfiltration.
Starting in July 2025, Interlock deployed a new remote access trojan (RAT) through a variation of the ClickFix technique called "FileFix". Execution and persistence rely on four distinct variants of the custom RAT. The group's evolving tactics and strategic integration of social engineering demonstrate a high level of operational maturity.

Social Engineering Evolution-ClickFix and FileFix

Technical exploitation requires significant resource expenditure. Human manipulation provides a cheaper, vastly more reliable entry vector. The threat ecosystem witnessed a massive transition away from complex exploit kits toward social engineering techniques designed to trick users into infecting their own machines. ClickFix emerged in late 2023 and rapidly became the dominant initial access method by 2025, accounting for 47 percent of observed attacks according to Microsoft's Digital Defense Report.
ClickFix relies entirely on human-assisted execution. Attackers compromise legitimate websites, utilizing JavaScript to present fake human verification lures. Victims encounter simulated browser crashes, fake Cloudflare CAPTCHA challenges, or full-screen Blue Screen of Death (BSOD) pages. The malicious webpage instructs the victim to copy a specific command to fix the fabricated error.

JavaScript automatically places a heavily obfuscated PowerShell script into the victim's clipboard. The page then instructs the user to open the Windows Run dialog or a system terminal and paste the contents. When the user executes the command, the script abuses legitimate Living-off-the-Land binaries (LOLBins) such as MSBuild.exe to compile and execute malicious project files entirely in memory. The payload typically disables real-time monitoring within Windows Defender before downloading a remote access trojan. The attack bypasses standard endpoint detection mechanisms because the user manually initiates the execution through trusted system utilities.

In June 2025, researchers identified a sophisticated evolution of the technique dubbed "FileFix". Threat actors adapted the methodology to avoid the Windows Run dialog, recognizing that many organizations disable the feature via Group Policy. FileFix silently launches a legitimate File Explorer window via a hidden HTML element. The webpage instructs the victim to paste a required file path directly into the Explorer address bar.

Once the victim hits the enter key, the malicious PowerShell command executes seamlessly,

downloading malware without generating visible system warnings. The Interlock ransomware group aggressively adopted FileFix to distribute its custom remote access trojan, demonstrating how rapidly advanced social engineering techniques permeate the cybercriminal underground. Defending against copy-paste social engineering requires comprehensive user awareness training and the strict restriction of PowerShell execution capabilities for non-privileged accounts.

Supply Chain Weaponization-The TamperedChef Campaign

Trojanized freeware serves as a primary precursor to ransomware deployment. The TamperedChef campaign exemplifies the extreme stealth and patience exhibited by modern initial access brokers. Operators used Search Engine Optimization (SEO) poisoning and malicious Google Ads to distribute fake PDF editing utilities and product manuals.

To bypass SmartScreen filters and antivirus heuristics, the TamperedChef installers were signed with legitimate Extended Validation certificates. Threat actors acquired the certificates through United States-based shell companies, including Stratus Core Digital LLC and DataX Engine LLC, granting the malicious applications immediate cryptographic trust from the operating system.
TamperedChef employed a strict 56-day dormancy period. During the hibernation phase, the fake applications functioned exactly as advertised, allowing users to edit PDFs without issue. The prolonged delay ensured the malware evaded dynamic sandbox analysis and bypassed standard incident response log retention windows. The malware covertly established persistence mechanisms by creating scheduled tasks designed to execute hidden JavaScript backdoors.

On August 21, 2025, operators triggered the payload across infected systems simultaneously using a specific command-line flag (--fullupdate). The backdoor ran silently in the background, forcibly terminating browser processes to unlock database files. The malware abused the Windows Data Protection API (DPAPI) to decrypt stored passwords, session cookies, and authentication tokens.

The stolen data was transmitted to attacker-controlled command-and-control servers using XOR encryption with randomized keys to obfuscate the exfiltration traffic. Access obtained through TamperedChef frequently led to secondary deployments of Akira, Qilin, and INC ransomware. The campaign demonstrates how legitimate software distribution channels frequently act as the vanguard for enterprise encryption events.

TeamPCP and Developer Infrastructure Compromise

The exploitation of trusted integrations extends far beyond simple malvertising. The TeamPCP supply chain attack executed in March 2026 illustrates the catastrophic downstream impact of compromised developer infrastructure. Threat actors systematically targeted open-source vulnerability scanners and continuous integration tools, embedding backdoors directly into the software supply chain.

TeamPCP compromised the Trivy vulnerability scanner via a misconfigured GitHub Actions workflow, resulting in CVE-2026-33634. Attackers stole continuous integration secrets, force-pushed malicious binaries starting with version v0.69.4, and poisoned GitHub Actions with an information stealer designed to harvest cloud tokens and Secure Shell (SSH) keys. The threat demonstrated worm-like propagation, spreading through compromised Node Package Manager (npm) packages and insecure Kubernetes Application Programming Interfaces (APIs). The campaign rapidly expanded to Checkmarx infrastructure, modifying the ast-github-action and kics-github-action workflows to collect repository secrets during pipeline execution. Finally, the actors targeted LiteLLM, a widely used proxy for large language models. By publishing poisoned packages on the Python Package Index (PyPI), attackers ensured execution upon installation via a maliciously crafted .pth file. The payload harvested database credentials and API keys for major artificial intelligence providers, completely compromising the downstream software environments.

Railway PaaS and OAuth Device Code Abuse

Threat actors relentlessly abuse legitimate Platform-as-a-Service (PaaS) providers to bypass geographic blocking and IP reputation filtering. The "Riding the Rails" campaign involved attackers hosting phishing infrastructure on Railway PaaS. Railway provides a trusted cloud platform with valid IP addresses, allowing malicious activity to blend seamlessly with normal corporate traffic.

The operation abused the OAuth device code flow to trick victims into providing authentication codes. Threat actors utilized personalized phishing lures delivered through multi-hop redirect chains, leading victims to official Microsoft login endpoints. Once a victim submitted a code, the threat actors received valid access and refresh tokens.

The tokens granted persistent access to Microsoft 365 resources without ever requiring the victim's password. Refresh tokens were continuously reused to generate new access tokens. The EvilTokens phishing-as-a-service platform powered the campaign, affecting hundreds of organizations globally. Mitigating such attacks requires the explicit disabling of device code flows within Conditional Access policies unless strictly necessary for specific hardware deployments.

The Scattered Lapsus$ Hunters (SLSH) Coalition

The Scattered Lapsus$ Hunters (SLSH) collective redefined cyber extortion in late 2025. Operating as a syndicate comprising members from Scattered Spider, ShinyHunters, and LAPSUS$, the group executed a massive supply chain compromise targeting cloud-based customer relationship management platforms. The operation completely bypassed traditional endpoint encryption, focusing entirely on data exfiltration and Extortion-as-a-Service.
The attack sequence commenced with the compromise of Salesloft GitHub repositories between March and June 2025. Attackers successfully extracted OAuth tokens associated with the Drift integration. Armed with valid programmatic tokens, SLSH accessed hundreds of Salesforce customer environments, bypassing multi-factor authentication and identity verification checks entirely.

Once inside the target environments, operators executed massive Salesforce Object Query Language (SOQL) queries. The queries targeted accounts, opportunities, support cases, and embedded secrets, including Amazon Web Services (AWS) keys and Snowflake tokens. The blast radius encompassed over 700 organizations, resulting in the theft of approximately one billion records from entities including FedEx, Disney, Home Depot, and Toyota.
SLSH operates a highly aggressive extortion portal designed to maximize public humiliation. On October 3, 2025, the group demanded a blanket ransom directly from Salesforce, threatening to leak the stolen data if the software provider refused to pay. Salesforce declined to negotiate. In response, international law enforcement agencies, including the Federal Bureau of Investigation, seized the group's clearnet domains on October 9. The collective immediately retreated to their darknet mirrors, released partial datasets to prove authenticity, and continued the extortion campaign unhindered.
In a disturbing tactical evolution, SLSH began recruiting female callers for synchronous voice phishing (vishing) campaigns. Offering upfront payments ranging from $500 to $1,000 per successful call, the group actively sought to bypass traditional attacker profiles recognized by IT help desk personnel. Female voices frequently circumvent the subconscious biases of support staff trained to anticipate aggressive, male-dominated social engineering attempts. The strategy demonstrates a profound understanding of human psychology and the vulnerabilities inherent within corporate support structures.

ShinySp1d3r and In-House Encryptor Evolution

SLSH announced the development of their own Ransomware-as-a-Service platform dubbed "ShinySp1d3r". The custom encryptor relies on the ChaCha20 algorithm and includes planned support for Linux and VMware ESXi environments. The transition from pure extortion to developing bespoke encryption tooling indicates a maturation of the collective's technical capabilities, ensuring they remain a paramount threat throughout 2026.

The ShinySp1d3r encryptor includes functionality to delete Volume Shadow Copies on infected endpoints, disable selected system services, and propagate automatically to other endpoints on the local network. Developing a standalone ransomware encryptor grants SLSH a secure, proprietary platform to conduct sophisticated attacks. The group threatens to deploy the encryptor against critical infrastructure, specifically mentioning New York State networks.

SLSH continues its strategy of recruiting insiders, offering massive payments for direct access to corporate networks. Following an incident involving a former CrowdStrike employee who provided internal screenshots and Single Sign-On (SSO) authentication cookies to the group via Telegram, the risk of insider threats escalated dramatically. Organizations must implement strict insider risk management protocols and monitor offboarding processes to prevent unauthorized access.

LockBit's Return and RaaS Market Dynamics

The once-prolific LockBit group reemerged in late 2025, attempting to reestablish its dominance within the threat ecosystem. LockBit 5.0 appeared on the RAMP dark web forum in September 2025, marking the group's six-year anniversary. The latest variant features numerous code overlaps with LockBit 4.0, integrating advanced anti-analysis features and appending unique

16-character extensions to encrypted files.
Despite the technical upgrades, LockBit struggles to regain its former market share. International law enforcement disruptions in 2024 severely damaged the brand's reputation among affiliates. The sanctions placed against Dmitry Khoroshev, the primary developer and administrator of the LockBit RaaS, create a substantial legal barrier for victims contemplating payment. Affiliates increasingly migrate to newer, more reliable syndicates like Qilin and Akira, recognizing the liability associated with the LockBit brand.

World Leaks emerged as another prominent player, directly replacing the Hunters International ransomware group. Hunters International publicly announced its retirement in late 2024, citing increased pressure from global law enforcement. World Leaks adopted a pure extortion model, abandoning encryption entirely in favor of custom exfiltration tooling. The group relies on SOCKSv5 proxies and Tor-based communications to extract massive volumes of data silently.

Despite claims of abandoning encryption, forensic analysis revealed World Leaks executing attacks that involved both data exfiltration and the deployment of ransomware payloads. The discrepancy highlights the fluid and deceptive nature of cybercriminal operations. Threat actors routinely alter their stated methodologies when lucrative opportunities arise.

Living-Off-The-Land and Evasion Tactics

Ransomware intrusions in 2025 demonstrated a high degree of tooling convergence. Threat actors relied heavily on legitimate, dual-use, and commodity tools across all phases of the attack lifecycle. Rather than developing bespoke malware, affiliates prioritized applications that blend into enterprise environments, complicating detection efforts.
Remote access tools dominated attacker toolkits. AnyDesk remained the most frequently observed utility, followed closely by ScreenConnect, Splashtop, TeamViewer, and RustDesk. Because IT teams routinely use these applications, ransomware actors manipulate them to maintain persistent, hands-on-keyboard access without triggering security alerts.
For credential access, Mimikatz remained highly effective at extracting NTLM hashes and Kerberos tickets from compromised systems. Network discovery tools like Advanced IP Scanner and NetScan allowed attackers to map victim environments rapidly. Threat actors deployed MegaSync and AzCopy for high-volume data exfiltration, transferring files directly to attacker-controlled cloud storage.
Defense evasion tactics grew increasingly aggressive. Attackers deployed Endpoint Detection and Response (EDR) killer tools, including Terminator, EDRKillShifter, Hotta Killer, and AVKiller malware. Bring-Your-Own-Vulnerable-Driver (BYOVD) techniques became standardized across the ecosystem. Attackers abused vulnerable drivers such as rwdrv.sys, K7RKScan.sys, and SysMon.sys to disable kernel-level protections entirely.
Command-and-control operations evolved to utilize Cloudflared and OpenSSH for establishing encrypted outbound tunnels. Advanced syndicates deployed frameworks like Cobalt Strike and Velociraptor for post-exploitation coordination. SystemBC functioned as a widely used proxy and remote access trojan, supporting encrypted communications and SOCKS5 proxying across both Windows and Linux environments.

The Threat Trajectory for 2026

The cyber extortion theater will experience further fragmentation and extreme specialization throughout 2026. Extortion-only models will dominate as threat actors recognize the operational efficiency of pure data theft over complex, easily detectable encryption routines. World Leaks established the definitive blueprint for pure extortion, minimizing technical friction while maximizing reputational damage and regulatory pressure.
Ransomware operations will continue to exploit edge-facing vulnerabilities and software supply chain weaknesses relentlessly. Tools like the AdaptixC2 framework, originally designed for legitimate penetration testing, will increasingly replace bespoke malware. The aggressive abuse of dual-use open-source security tools complicates attribution efforts and easily evades standard signature-based detection mechanisms.

Organizations must comprehensively discard obsolete perimeter-based defense paradigms. Identity represents the new perimeter. Securing modern enterprise environments requires aggressive token management, the immediate revocation of unnecessary OAuth grants, and the strict enforcement of Conditional Access policies. Defenders must transition from reactive incident response to proactive identity posture management, assuming breach as a baseline operational reality rather than a theoretical anomaly. Failure to adapt to the industrialized scale of modern cybercrime ensures inevitable compromise, severe financial degradation, and irreversible reputational ruin.

Works cited

1. Darktrace Identifies Encryption in a World Leaks Ransomware Attack, https://www.darktrace.com/blog/when-reality-diverges-from-the-playbook-darktrace-identifies-encryption-in-a-world-leaks-ransomware-attack 2. Telefonica Tech · Blog - Telefónica Tech, https://telefonicatech.com/en/blog/author/telefonicatech 3. Crypto Ransomware: 2026 Crypto Crime Report - Chainalysis, https://www.chainalysis.com/blog/crypto-ransomware-2026/ 4. Ransomware Payments Decline 8% as Attacks Surge 50% - Infosecurity Magazine, https://www.infosecurity-magazine.com/news/ransomware-payments-decline-1/ 5. Cyber risk and cybersecurity: a systematic review of data availability - PMC, https://pmc.ncbi.nlm.nih.gov/articles/PMC8853293/ 6. Cybersecurity: Impact on Insurance Business and Operations - SOA, https://www.soa.org/globalassets/assets/files/static-pages/sections/joint-risk-mgmt/cyber-security-impact.pdf 7. An Analytical Review of Cyber Risk Management by Insurance Companies: A Mathematical Perspective - MDPI, https://www.mdpi.com/2227-9091/13/8/144 8. Ransomware Statistics, Data, Trends, and Facts [updated 2026] - Varonis, https://www.varonis.com/blog/ransomware-statistics 9. Overcoming Biases in Cyber Security Problem Analysis and Decision-Making, https://cybersecurity-magazine.com/overcoming-biases-in-cyber-security-problem-analysis-and-decision-making/ 10. A Threat Intelligence Analyst's Guide to Today's Sources of Bias - ReliaQuest, https://reliaquest.com/blog/a-threat-intelligence-analysts-guide-to-todays-sources-of-bias/ 11. Iterative Analysis of Competing Hypotheses to Overcome Cognitive Biases in Cyber Decision-Making | Journal of Information Warfare, https://www.jinfowar.com/journal/volume-17-issue-2/iterative-analysis-competing-hypotheses-overcome-cognitive-biases-cyber-decision-making 12. Mastering the Analysis of Competing Hypotheses (ACH): A Practical Framework for Clear Thinking - SOS Intelligence, https://sosintel.co.uk/mastering-the-analysis-of-competing-hypotheses-ach-a-practical-framewor

k-for-clear-thinking/ 13. Analysis of Competing Hypotheses - Rodolfo Santos Flaborea - Medium, https://anticitizenone.medium.com/analysis-of-competing-hypotheses-176bd8147dbc 14. World Leaks Ransomware - Blackpoint Cyber, https://blackpointcyber.com/threat-profile/world-leaks-ransomware/ 15. The Golden Scale: Bling Libra and the Evolving Extortion Economy, https://unit42.paloaltonetworks.com/scattered-lapsus-hunters/ 16. World Leaks Data Extortion: What You Need to Know - Fortra, https://www.fortra.com/blog/world-leaks-data-extortion-what-you-need-know 17. Ransomware payments dropped in 2025 as attack numbers reached record levels: Chainalysis - Therecord.media, https://therecord.media/ransomware-payments-chainalysis-cybercrime 18. 2026 Ransomware and Cyber Threat Report | GuidePoint Security, https://www.guidepointsecurity.com/wp-content/uploads/2026/01/GRIT-2026-Ransomware-and-Cyber-Threat-Report.pdf 19. SSL VPN vulnerability impacting Gen 7 SonicWall Firewalls (CVE-2024-40766) – Update 1 - Canadian Centre for Cyber Security, https://www.cyber.gc.ca/en/alerts-advisories/potential-ssl-vpn-zero-day-vulnerability-impacting-gen-7-sonicwall-firewalls 20. RaaS meets misconfiguration: How Akira is exploiting SonicWall SSLVPN weaknesses, https://www.threatlocker.com/blog/raas-meets-misconfiguration-how-akira-is-exploiting-sonicwall-sslvpn-weaknesses 21. Akira SonicWall Campaign Uncovered - Darktrace, https://www.darktrace.com/blog/inside-akiras-sonicwall-campaign-darktraces-detection-and-response 22. Dragos Industrial Ransomware Analysis: Q2 2025, https://www.dragos.com/blog/dragos-industrial-ransomware-analysis-q2-2025 23. Ransomware Statistics 2025: Latest Trends & Must-Know Insights - Fortinet, https://www.fortinet.com/resources/cyberglossary/ransomware-statistics 24. Akira ransomware: official decryptor 0 - technical expertise 1, https://sosransomware.com/en/ransomware-en/akira-ransomware-official-decryptor-0-technical-expertise-1/ 25. The DragonForce Cartel: Scattered Spider at the gate - Acronis, https://www.acronis.com/en/tru/posts/the-dragonforce-cartel-scattered-spider-at-the-gate/ 26. Ransomware Trends In May 2025 - Cyber Security Intelligence, https://www.cybersecurityintelligence.com/blog/ransomware-trends-in-may-2025-8499.html 27. Ransomware 2025: A Resilient and Persistent Threat - SECURITY.COM, https://www.security.com/sites/default/files/2025-02/2025_02_Ransomware_2025.pdf 28. The Evolution of Qilin RaaS - SANS Institute, https://www.sans.org/blog/evolution-qilin-raas 29. Worldwide outage at X due to DDoS attack | Cyber Intelligence Briefing: March 14, 2025, https://www.s-rminform.com/en-us/cyber-intelligence-briefing/cyber-intelligence-briefing-14-march-2025 30. Moonstone Sleet, Storm-1789, Group G1036 - MITRE ATT&CK®, https://attack.mitre.org/groups/G1036/ 31. Extortion and Ransomware Trends January-March 2025 - Unit 42, https://unit42.paloaltonetworks.com/2025-ransomware-extortion-trends/ 32. Cyber Threat Feed: Latest Advisories And Intelligence - Cybercrime Magazine, https://cybersecurityventures.com/esentire-blog/ 33. Threat Actors Deploy Sinobi Ransomware via Compromised SonicWall SSL VPN Credentials | eSentire, https://www.esentire.com/blog/threat-actors-deploy-sinobi-ransomware-via-compromised-sonicwall-ssl-vpn-credentials 34. TRACKING RANSOMWARE : JUNE 2025 - CYFIRMA, https://www.cyfirma.com/research/tracking-ransomware-june-2025/ 35. The State of Ransomware – Q3 2025 - Check Point Research, https://research.checkpoint.com/2025/the-state-of-ransomware-q3-2025/ 36. The State of Ransomware in the U.S.: Report and Statistics 2025 2025 Ransomware Statistics - Emsisoft, https://www.emsisoft.com/en/blog/47215/the-state-of-ransomware-in-the-u-s-report-and-statistic

s-2025/ 37. Ransomware Landscape in H2 2025: Statistics and Key Issues - S2W – Medium, https://s2w.medium.com/ransomware-landscape-in-h2-2025-statistics-and-key-issues-079ebd4fbbfa 38. Dragos Industrial Ransomware Analysis: Q3 2025, https://www.dragos.com/blog/dragos-industrial-ransomware-analysis-q3-2025 39. Dark Web Profile: Sinobi Ransomware - SOCRadar, https://socradar.io/blog/dark-web-profile-sinobi-ransomware/ 40. Sinobi ransomware: the extortion group that relies on stealth and exclusivity, https://sosransomware.com/en/ransomware-groups/sinobi-ransomware-successor-to-lynx-and-inc/ 41. Keep up with Ransomware, https://assets.ctfassets.net/6hqdqj4fjyeg/2tltEY0aWYBfHtJxDl5FV1/0d260b7112330cab549a9337d3ec5ce7/2._Keep_up_with_Ransomware_Jan_Sinobi_Ransomware_Analysis_of_Lynx_Group_Ties.pdf 42. Sinobi Ransomware - Blackpoint Cyber, https://blackpointcyber.com/threat-profile/sinobi-ransomware/ 43. Clawdbot - Data Security Council of India (DSCI), https://www.dsci.in/files/content/advisory/2026/threat-advisory-january-2026.pdf 44. A Year Later, Interlock Ransomware Keeps Leveling Up - Forescout, https://www.forescout.com/blog/a-year-later-interlock-ransomware-keeps-leveling-up/ 45. ClickFix: The Evolution of Copy-Paste Social Engineering | Todyl, https://www.todyl.com/blog/clickfix-evolution-copy-paste-social-engineering 46. ClickFix: The Social Engineering Technique Hackers Use to Manipulate Victims | Group-IB Blog, https://www.group-ib.com/blog/clickfix-the-social-engineering-technique-hackers-use-to-manipulate-victims/ 47. Think before you Click(Fix): Analyzing the ClickFix social engineering technique - Microsoft, https://www.microsoft.com/en-us/security/blog/2025/08/21/think-before-you-clickfix-analyzing-the-clickfix-social-engineering-technique/ 48. Analyzing PHALT#BLYX: How Fake BSODs and Trusted Build Tools Are Used to Construct a Malware Infection - Securonix, https://www.securonix.com/blog/analyzing-phaltblyx-how-fake-bsods-and-trusted-build-tools-are-used-to-construct-a-malware-infection/ 49. Ongoing ClickFix Campaign - Cyber Security Agency of Singapore (CSA), https://www.csa.gov.sg/alerts-and-advisories/alerts/al-2025-068/ 50. ClickFix & FileFix: How a Copy-Paste Trick Became 2025's Top Social Engineering Threat, https://socradar.io/blog/clickfix-filefix-copy-paste-top-social-engineering/ 51. Trojan:HTML/FileFix.DSK!ams threat description - Microsoft Security Intelligence, https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Trojan:HTML/FileFix.DSK!ams 52. FileFix – The Evolved ClickFix - Bridewell, https://www.bridewell.com/insights/blogs/detail/filefix-the-evolved-clickfix 53. New FileFix Delivery Method Used to Distribute Interlock RAT - Arctic Wolf, https://arcticwolf.com/resources/blog-uk/new-filefix-delivery-method-used-to-distribute-interlock-remote-access-trojan/ 54. FileFix: The New Social Engineering Attack Building on ClickFix Tested in the Wild, https://blog.checkpoint.com/research/filefix-the-new-social-engineering-attack-building-on-clickfix-tested-in-the-wild/ 55. Click-Fix Attacks Now Using Fake Blue Screen of Death - Arete Incident Response, https://areteir.com/resources/clickfix-fake-bsod-attacks-target-hospitality 56. TamperedChef serves bad ads, with infostealers as the main course | SOPHOS, https://www.sophos.com/en-us/blog/tamperedchef-serves-bad-ads-with-infostealers-as-the-main-course 57. TamperedChef: A High-Severity Multi-Stage Infostealer Operation - Hive Pro, https://hivepro.com/threat-advisory/tamperedchef-a-high-severity-multi-stage-infostealer-operation/ 58. Dataprise Defense Digest: TamperedChef Malware Campaign, https://www.dataprise.com/resources/defense-digest/tampered-chef-malware-campaign/ 59.

Malicious Appsuite PDF Editor Spreads Tamperedchef Malware - Truesec, https://www.truesec.com/hub/blog/tamperedchef-the-bad-pdf-editor 60. Campaign Exploiting SimpleHelp RMM Software for Initial Access ..., https://arcticwolf.com/resources/blog/arctic-wolf-observes-campaign-exploiting-simplehelp-rmm-software-for-initial-access/ 61. Cybersecurity Trends 2026 - IBM, https://www.ibm.com/think/insights/more-2026-cyberthreat-trends 62. Scattered LAPSUS$ Hunters: 2025's Most Dangerous Cybercrime Supergroup, https://www.picussecurity.com/resource/blog/scattered-lapsus-hunters-2025s-most-dangerous-cybercrime-supergroup 63. Scattered Lapsus$ Hunters Launch Data Leak Site Targeting Salesforce: Massive OAuth Supply Chain Breach Exposes 1 Billion Records - Rescana, https://www.rescana.com/post/scattered-lapsus-hunters-launch-data-leak-site-targeting-salesforce-massive-oauth-supply-chain-bre 64. A Full Recap of Salesforce Supply-Chain Nightmare: How One Breach Impacted 700+ Organizations - NetSecurity.com, https://www.netsecurity.com/a-full-recap-of-salesforce-supply-chain-nightmare-how-one-breach-impacted-700-organizations/ 65. ShinyHunters Wage Broad Corporate Extortion Spree - Krebs on Security, https://krebsonsecurity.com/2025/10/shinyhunters-wage-broad-corporate-extortion-spree/ 66. Scattered Lapsus$ resurfaces with brokered access model, raising risks for industrial and critical infrastructure, https://industrialcyber.co/ransomware/scattered-lapsus-resurfaces-with-brokered-access-model-raising-risks-for-industrial-and-critical-infrastructure/ 67. INDUSTRY ARTICLES - Cubex Group, https://cubexgroup.com/industry-articles/ 68. Scattered Lapsus$ Hunters seeks women for vishing attacks - Help Net Security, https://www.helpnetsecurity.com/2026/02/26/slh-seeks-women-for-vishing-attacks/ 69. Scattered Lapsus$ Hunters Recruiting Women for Operations - Dataminr, https://www.dataminr.com/resources/intel-brief/slh-recruiting-women-for-vishing/ 70. How Scattered LAPSUS$ Hunters Illustrates the Evolution of Cybercrime - Dataminr, https://www.dataminr.com/resources/blog/how-scattered-lapsus-hunters-illustrates-the-evolution-of-cybercrime/ 71. Threat Actor Spotlight - ShinySp1d3r - MOXFIVE, https://www.moxfive.com/resources/moxfive-threat-actor-spotlight-shinysp1d3r 72. ShinySp1d3r Ransomware - Broadcom Inc., https://www.broadcom.com/support/security-center/protection-bulletin/shinysp1d3r-ransomware 73. Flash Report: Powerful New RaaS from Scattered Lapsus$ Hunters | ZeroFox, https://www.zerofox.com/intelligence/flash-report-powerful-new-raas-from-scattered-lapsus-hunters/ 74. Cyber Security Weekly Briefing, 22-28 November - Telefónica Tech, https://telefonicatech.com/en/blog/cyber-security-briefing-%2022-28-november-2025 75. Exaforce Blog | SOC insights, incident analysis, and product innovation, https://www.exaforce.com/blogs 76. Ransomware Trends & Data Insights: January 2026 - Arete Incident Response, https://areteir.com/resources/ransomware-trends-data-insights-january-2026 77. Top 10 Critical Threat Actors to Watch in 2026: Ransomware, APTs & Defensive Strategies, https://netlas.io/blog/top_10_critical_threat_actors/ 78. Interlock Ransomware: New Techniques, Same Old Tricks | FortiGuard Labs - Fortinet, https://www.fortinet.com/blog/threat-research/interlock-ransomware-new-techniques-same-old-tricks 79. Ransomware Didn't Slow Down in Q4. Here's What That Means for 2026. | ZeroFox, https://www.zerofox.com/blog/ransomware-didnt-slow-down-in-q4-heres-what-that-means-for-2026/ 80. World Leaks - Blackpoint Cyber, https://blackpointcyber.com/wp-content/uploads/2026/01/World-Leaks.pdf 81. Russian Ransomware Groups Exploit AdaptixC2: Advanced Attacks Targeting Windows, Linux, and

macOS Systems - Rescana,
https://www.rescana.com/post/russian-ransomware-groups-exploit-adaptixc2-advanced-attacks-targeting-windows-linux-and-macos-sy 82. Analyzing "Scattered Lapsus$ Hunters" breaches since 2021 - Push Security, https://pushsecurity.com/blog/scattered-lapsus-hunters 83. FileFix in the wild! New FileFix campaign goes beyond POC and leverages steganography,
https://www.acronis.com/en/tru/posts/filefix-in-the-wild-new-filefix-campaign-goes-beyond-poc-and-leverages-steganography/