Most Noteworthy **Cyber Attacks** of 2025 (so far)

Santosh Pandit

20 July 2025

Important Disclaimer: All views in this paper are entirely my own and may not be necessarily shared by my employer or other cyber experts. Cyber risk is a complex beast, and no single person or organisation knows everything. Research on previous cyber incidents is extremely difficult, and you should expect gaps and errors in this report. I am trying my best to add value to my readers.

Table of Contents

Backdrop

2025 has thus far been a year of contradictions. The volume of attacks appears to have decreased. My own servers are receiving fewer hits than last year. However, the sophistication of cyber-attacks has markedly increased this year. The Coinbase incident involved bribery and highlighted something we have observed on the darknet for many years. We witnessed several sophisticated attacks that resembled certain chess moves. They are difficult to detect until a grandmaster explains them to you.

The context for these sophisticated attacks was predictable even 12 months before they occurred. I can confidently say that my 2024 cyber predictions materialised more prominently in 2025.

Attack Types

The 2025 attacks exploit emerging technologies such as AI (and online LLMs), target overlooked vectors including cloud identities and firmware and employ adaptive evasion tactics that challenge conventional defences. Key themes include supply chain compromises for amplified impact, AI-enhanced personalisation and automation, malware-free intrusions, and long-term persistence strategies.

Whilst ransomware, phishing, and zero-day exploits remain prevalent, the innovation lies in their evolution: AI-driven scalability, exploitation of trusted tools and relationships (such as MSPs and insiders), and targeting of blind spots including edge devices and AI systems themselves.

Note that it is extremely difficult to conclude the details of each attack, as we still do not have the culture of transparency and information sharing. Also note, the attack none of us can confirm is the "harvest now, decrypt later" approach associated with quantum computers.

Noteworthy Attacks of 2025

I have grouped the 2025 attacks thematically for clarity, with a summary table of key incidents.

1. Supply Chain and Third-Party Attacks

Attackers increasingly targeted software ecosystems, vendors, and managed service providers (MSPs) to compromise multiple victims via trusted channels, demonstrating strategic patience with dormant payloads activated years later.

- **Magento E-Commerce Extensions Backdoor**: Cybercriminals inserted backdoors into 21 popular Magento plugins as early as 2019, activating them in April 2025 to affect 500–1,000 online stores, including a $40 billion multinational. This long-dormant compromise evaded detection by blending malicious code with legitimate updates. (Sources: SC-Media and BankInfoSecurity)
- **Gluestack NPM Packages Trojanisation**: In June 2025, 17 React Native libraries (with ~1 million weekly downloads) were updated with hidden remote-access Trojans, infecting developers and downstream apps before discovery. (Sources: SC-Media, SecurityBrief, and SecurityBrief)
- **SimpleHelp RMM Exploitation (DragonForce Ransomware)**: The DragonForce gang chained older vulnerabilities (e.g., CVE-2024-57727, CVE-2024-57728) in SimpleHelp remote-management tools to breach an MSP and cascade ransomware to customers, highlighting the cascading risks of RMM platforms. (Sources: MSSP Alert, SocRadar, Broadcom, and CVE Details)
- **VeraCore Warehouse Management Software (XE Group)**: The XE Group exploited zero-days since 2020, maintaining persistent webshells for espionage on manufacturing supply chains. (Sources: CyberSecurityDive, and CyberScoop)
- **General Supply Chain Sieges**: Incidents like the Change Healthcare breach and open-source backdoors (e.g., detected via unusual CPU spikes) amplified impact through vendor ecosystems, with AI accelerating vulnerability chaining. Note: I am aware that the breach occurred in 2024, but its repercussions were more obvious in 2025. (Sources: CyberSecurityDive, The HIPAA Journal, ETH Zurich, and SecureWorld)

Why Noteworthy: These attacks abuse trusted software and services for broad reach, often with years-long dormancy, bypassing endpoint security and emphasising the need for ecosystem-wide monitoring.

2. AI-Driven and Generative AI Abuse

AI has lowered barriers for attackers, enabling automated, hyper-personalised threats and even autonomous exploitation.

- **AI-Crafted Phishing and Deepfakes**: Generative AI created realistic voice/video impersonations for BEC scams, e.g., faking executives to authorise fraudulent transfers. Tools like Xbow autonomously discovered vulnerabilities in companies such as Disney, AT&T, and Ford. (Sources: ZeroThreat, JPMorgan, and Vipre). The sources for Xbow are AIinvest, ZytechDigital, and Xbow.

- **AI-Powered Malware Mutation and Agent Exploitation**: Polymorphic malware changes code in real-time to evade detection, while "Agentware" hijacks AI agents for tasks like data scraping or DoS attacks. (Sources for polymorphic malware: SecurityWeek, Cyber Defence Magazine, and TRMLabs) (Sources for Agentware are HiddenLayer, and UC Berkeley)
- **Living Off the AI (Prompt Injection)**: Attackers exploited AI systems directly, injecting malicious prompts to turn them into attack platforms. I must add that injection attacks are a decade old, but the AI context makes them noteworthy for 2025. (Sources: OWASP, and Paul M. Duvall)
- **Lowering Entry Barriers**: A few years ago, I would have laughed at the idea of mentioning less sophisticated attackers known as “script kiddies”. However, in 2025 AI tools empowered these "script kiddies" to craft custom malware, identify exploits, or generate phishing content faster. (Sources: Dev.to, UC Berkeley, and SC Media)

Why Noteworthy: AI shifts attacks from manual to automated and adaptive, democratising sophisticated capabilities and making social engineering more scalable and undetectable.

3. Zero-Day Exploits and Nation-State Campaigns

Please note that I am highly allergic to attribution of cyber-attacks to nation states and APTs. However, for this section I will refer to the attribution made by other experts.

State actors and criminals used undisclosed flaws for stealthy access, often in critical infrastructure or via chained vulnerabilities.

- **Commvault Azure Breach**: Attributed to a Chinese nation-state actor (Silk Typhoon), the hacker exploited CVE-2025-3928 to install webshells in Commvault's cloud backups. (Sources: Varonis, C. Oscar Lawshea, and New Jersey Gov)
- **SentinelOne Vendor Compromise (APT41)**: Attributed to the Chinese APT41. The hacker targeted SentinelOne via a trusted IT vendor, deploying the ShadowPad backdoor (obfuscated as "ScatterBrain") with timed delays, reboots for trace removal, and Nimbo-C2 for control. (Sources: SentinelOne, InfoSecurity Magazine, and Industrial Cyber)
- **Microsoft SharePoint Zero-Day Chain**: CVE-2025-53770 was chained with CVE-2025-49706 and CVE-2025-49704 for remote code execution on enterprise servers. (Sources: The Stack, NIST, and Trend Micro)
- **GPU Driver Zero-Days**: Qualcomm Adreno flaws were exploited on smartphones, expanding attacks to hardware layers. The concern is that GPU drivers, having direct access to memory with kernel privileges, offer a highly attractive target for attackers, enabling deep, privileged access to smartphones. (Sources: TechZine, and Recorded Future)

Why Noteworthy: Chaining zero-days with supply-chain pivots allows persistent, undetected access, even in high-security environments like cybersecurity firms.

4. Endpoint, EDR Bypass, and Malware Innovations

Techniques focused on subverting defences without new malware, using legitimate processes for evasion.

- **"Bring Your Own Installer" (BYOI) Bypass**: Attackers exploited SentinelOne's EDR update process to disable tamper protection and deploy Babuk ransomware, leveraging signed installers to "trick" the tool into self-unloading. To be more precise, the "trick" is to interrupt its legitimate upgrade process at a precise moment when its protections are momentarily offline, leaving the system vulnerable. (Sources: Halcyon, InfoSecurity Magazine, and AON)
- **Infostealers via Cracked Apps**: Lumma Stealer variants, distributed through fake keygens, stole live sessions for rapid follow-on attacks. This includes stealing session cookies from browsers. For my experimental platform (kyber.club) I spent almost a week perfecting the cookie security by attacking it. (Sources: Cloudflare Cloudforce, Microsoft Security, Cybereason, and Gen Digital)
- **Waiting Thread Hijacking**: Chinese actors (e.g., Mustang Panda) used MAVInject.exe for stealthy code execution in certain breaches. Sources say the breaches affected Hertz and Delhaize, but I cannot be sure. Mustang Panda uses the official Microsoft executable to inject malicious payloads into legitimate processes like waitfor.exe or explorer.exe, allowing their malware to execute under the guise of a trusted process, thus bypassing many EDR and antivirus solutions. (Sources: GrayLog, Asec, and InformationSecurity Magazine)

Why Noteworthy: These "malware-free" methods repurpose defender tools or processes, extending dwell time and complicating forensics.

5. Firmware, IoT, and Edge Device Attacks

Attackers moved deeper into hardware for persistence that survives updates and resets.

- **ASUS Router Botnet (AyySSHush)**: Over 9,000 routers were backdoored via NVRAM SSH key injection after exploiting CVE-2023-39780, disabling logs and leaving no visible malware files. The campaign was designed to be "malware-free" in the traditional sense, relying on legitimate router features and configuration changes to remain stealthy, making it difficult to detect with traditional EDR. (Sources: Field Effect, Grey Noise, and SC Media)
- **Pivoting Through Edge Devices**: Groups like Akira routed attacks via unmonitored IoT or appliances (e.g., Fortinet/Ivanti zero-days) to evade EDR. They used this compromised IoT device to mount Windows SMB shares and deploy their Linux-based ransomware encryptor, thereby bypassing EDR solutions that were not designed to monitor such devices. (Sources: Sumo Logic, Cyfirma, HIPAA journal, and PICUS)

Why Noteworthy: Targeting persistent memory and built-in features creates "invisible" backdoors, shifting threats beyond software to hardware blind spots.

6. Advanced Social Engineering and Human-Centric Attacks

Exploiting trust and fatigue remained key, with novel twists.

- **Insider Bribery (Coinbase Ransomware)**: Attackers bribed overseas support agents to access internal tools and steal user data. This incident showed the need for due diligence of staff and contractors throughout the supply chain. (Sources: Xcitium, Global Relay, CM Alliance, and there was another great article that I can't find now.)
- **MFA Exhaustion and Help Desk Targeting (Scattered Spider)**: Repeated MFA prompts wore down users, followed by privilege escalation via help desks. (Sources: CyberArk, Splunk, Halcyon, and SC Media)
- **Weaponised GitHub and Fake Interviews (Water Curse)**: Malicious "pen-testing" tools or job challenges delivered malware to developers. By the way, another variation of the Fake Interviews is also the "paid consultation" scam where they offer you 300 pounds for an hour with their "customer". (Sources: There are quite a few on GitHub, the one from Cyware is good. For fake jobs - CyberSecurityDive and Tecnica)
- **ClickFix Attacks (iClicker)**: Fake CAPTCHA prompts tricked users into installing malware on educational platforms. (Sources: University of Michigan, Kaspersky, and Blackwired)

Why Noteworthy: Blends technical exploits with psychological manipulation, including insider recruitment and fatigue-based tactics.

7. Ransomware and Financial Manipulation Evolutions

Ransomware added destructive elements and new models.

- **Akira with Wiper Module**: While Akira ransomware has been known for its double-extortion model (encryption + data exfiltration) since its emergence in March 2023, reports from May/June 2025 indeed confirm its evolution to include a wiper module, creating "extinction-level" events. This means that even if a victim pays the ransom, the data could still be destroyed, eliminating the incentive for payment and turning the attack into pure sabotage. This reminds me of those idiots of Darkside Kingdom, whose encryption was so rubbish that their own decryption key failed to work. (Sources: Halcyon, Intertec, and Checkpoint)
- **RaaS Enhancements (RansomHub)**: The APT RansomHub was already active in 2024, and such emerging groups offered affiliate models for data ransom or access sales. Overall, I find that the new APTs created over the last 2-3 years have picked up momentum in 2025. (Sources: Masked Actors, Checkpoint, and Halcyon)
- **Cryptocurrency Market Manipulation**: Japan's FSA reported $2 billion in unauthorised trades via compromised accounts. (Sources: Recorded Future, Japanese FSA, and another article from Recorded Future)

Why Noteworthy: Wiper integration escalates stakes, while RaaS democratises attacks.

8. Other Emerging Vectors

- **Malware-Free Cloud Intrusions**: Exploiting OAuth tokens and APIs for "living-off-the-cloud" access in platforms like Microsoft 365.
- **Quantum-Enabled Threats**: "Harvest now, decrypt later" strategies anticipate breaking encryption. I have always emphasised the need to improve end-to-end encryption including the network connectivity. In addition, DNSSEC will play a greater role in the future.
- **Hacktivist DDoS via Telegram**: Groups like NoName057 coordinated infrastructure disruptions through encrypted channels.

Summary of Key Incidents

Attack Case	Attacker Type	Target	Technique	Innovative Aspect
Magento Extensions Backdoor	Cybercriminal	E-commerce stores	Dormant supply-chain trojans	Long-term (6+ years) activation in trusted plugins.
SimpleHelp RMM (DragonForce)	Cybercriminal	MSPs and customers	Vulnerability chaining in RMM tools	Cascading ransomware via managed services.
SentinelOne Vendor Breach (APT41)	Nation-state (China)	Cybersecurity firm	Supply-chain backdoor with evasion (delays, reboots)	Multi-stage stealth against security vendors.
BYOI EDR Bypass	Cybercriminal (Babuk)	Endpoints with SentinelOne	Exploit update process	Subverts legitimate installers to disable defences.
ASUS Router Botnet (AyySSHush)	Advanced attackers	Home routers	NVRAM firmware backdoor	Persistent, malware-free SSH access surviving updates.
AI Deepfakes and Xbow	Cybercriminal/AI tools	Businesses (e.g., Disney)	Generative AI for phishing/vuln discovery	Autonomous, personalised attacks at scale.
SharePoint Zero-Day Chain	Cybercriminal	Enterprise servers	Chained vulnerabilities for RCE	Rapid weaponisation of unpatched enterprise software.
Insider Bribery (Coinbase)	Cybercriminal	Cryptocurrency exchange	Financial incentives to employees	Direct recruitment for internal access.

How do defend?

Let us discuss over a coffee.

Santosh Pandit

Copyright © 2025

License: CC BY (Creative Commons with Attribution)