TIR-20251231 End-of-the-Year Recap 2025

12/31/2025

Prepared for:

Aspire Technology Partners
25 James Way
Eatontown, NJ 07724

NOTICE:

This document is marked TLP: CLEAR, allowing recipients to share this information globally without any disclosure limitations.

This report is governed by the terms outlined in the Master Services Agreement (MSA) or any other master agreement between Aspire Technology Partners and the client receiving this report, along with the Statement of Work (SOW) or Order detailing the services that led to its creation.

Contributor(s)

Portia S. Cole
CTI Threat Researcher
Aspire Technology Partners
pcole@aspiretransforms.com

TABLE OF CONTENTS

Executive Summary 3
Top Vulnerabilities and Campaigns of 2025 4
Top Threat Actors of 2025 10
Aspire's Predictions for 2026 15
Conclusion 16
Aspire Protects 17
Supporting Documentation 18
Appendix II: Disclaimer 19

Executive Summary

In 2025, attackers focused on the systems that keep organizations running. Network devices, virtualization platforms, identity-linked services, and core operating system components were targeted because compromise at those layers gave attackers control that spread quickly. Cisco, VMware, Fortinet, Microsoft, and trusted Software-as-a-Service (SaaS) integrations showed up repeatedly in intrusion chains. Not because they were ignored, but because failures at those points had immediate impact. Once inside these systems, attackers often maintained access for long periods of time, with activity that was hard to spot and difficult to remove.

Ransomware and extortion activity followed the same pattern. The most active groups did not rely on novelty or constant reinvention. Instead, they refined access paths and reused tooling. Groups like Qilin and Play were laser focused on volume and repeatability, while others such as Medusa and Akira focused on pressure through data theft and infrastructure disruption.

Scattered Spider showed that malware was optional when identity systems could be manipulated, and CL0P demonstrated that a single supply-chain exploit could outweigh months of traditional ransomware operations. Across these campaigns, encryption was often secondary to data theft and delayed extortion.

Attackers stopped chasing endpoints in 2025. They went after management layers and identity systems instead. Those access paths

TIR SUMMARY

ASPIRE

TLDR;

- Attackers in 2025 focused on systems that sit at the center of the environment, not individual endpoints.
- Network devices, virtualization platforms, identity systems, and trusted SaaS integrations showed up repeatedly in real intrusions.
- Many high-impact attacks relied on known vulnerabilities and exposed systems rather than new exploits.
- Ransomware groups scaled through repeatable access paths and affiliate growth, not new techniques.
- Data theft mattered more than encryption in many campaigns, with pressure applied over time instead of immediate lockouts.
- Identity abuse worked without malware through social engineering, helpdesk manipulation, MFA fatigue, and SSO abuse.
- Supply-chain and SaaS access delivered wide impact quickly and often bypassed traditional security alerts.
- The same access paths remain open heading into 2026, making a change in attacker behavior unlikely unless those gaps close.

worked then and they are still working now. Let's take a look back at 2025 and get ready for what's to come.

Top Vulnerabilities and Campaigns of 2025

The vulnerabilities and campaigns that mattered most in 2025 shared one thing in common - they hit the layers organizations trust to keep everything running. Attackers repeatedly went after network devices, virtualization platforms, identity-linked services, and core Windows components, knowing that a single weakness at those layers could open entire environments.

Some of the activity centered on new zero-days, while other campaigns leaned on flaws that had been public for years but remained exposed. The sections below break down the specific vulnerabilities and intrusion campaigns that defined the year for many organizations. You will see how vulnerabilities were exploited, what systems were put at risk, and why these issues kept appearing in attacks long after patches were available.

Cisco

Cisco vulnerabilities stood out in 2025 due to their consistent exploitation against core network and security infrastructure. Rather than targeting user endpoints, attackers focused on devices that control traffic flow, authentication, and visibility across enterprise environments.

Firewalls, routers, switches, and email security appliances running Cisco software were repeatedly abused through both new zero-days and old flaws, many of which provided root-level access. These vulnerabilities gave attackers durable control over trusted systems and, in several cases, supported long-term access tied to espionage and large-scale intrusion campaigns.

Cisco Vulnerabilities Exploited in 2025

- CVE-2025-20393, CVSS 10 (Cisco Secure Email Gateway / Secure Email and Web Manager) – A zero-day in AsyncOS that allowed unauthenticated attackers to execute operating system commands as root when the Spam Quarantine feature was exposed to the internet. Exploitation led to full appliance compromise, persistent backdoors, and access to email traffic.

- CVE-2025-20333, CVSS 9.9 (Cisco ASA / FTD) – A vulnerability in the VPN web server that allowed attackers with valid VPN credentials to execute arbitrary code

as root on the firewall itself. Successful exploitation resulted in full device takeover at the network edge.

- CVE-2025-20362, CVSS 6.2 (Cisco ASA / FTD) – A related flaw in the VPN web server that allowed unauthenticated access to restricted URLs. While less severe on its own, it weakened firewall access controls and supported broader exploitation activity.

- CVE-2017-6736, CVE-2017-6737, CVE-2017-6738, CVSS 8.8 (Cisco IOS / IOS XE SNMP) – Long-standing SNMP buffer overflow vulnerabilities that remained exploitable due to unpatched systems and exposed SNMP services. Attackers could crash devices or gain remote control using crafted SNMP packets, reinforcing how legacy flaws continued to drive real-world impact.

- CVE-2018-0171, CVSS 9.8 (Cisco IOS / IOS XE Smart Install) – A Smart Install vulnerability that allowed remote code execution on exposed devices. This flaw continued to surface in intrusion activity years after disclosure, particularly in large-scale network environments.

- CVE-2023-20198 and CVE-2023-20273, CVSS 10 (Cisco IOS XE Web UI) – Web UI privilege escalation vulnerabilities that allowed attackers to gain administrative access to affected devices. These flaws were repeatedly abused to escalate control once management interfaces were reachable.

- CVE-2024-20399, CVSS 6 (Cisco NX-OS) – A command injection issue in NX-OS that allowed attackers to execute unauthorized CLI commands, affecting high-end switching infrastructure used in data centers and telecom networks.

VMware

Virtualization infrastructure sat squarely in attackers' sights throughout 2025, with VMware platforms repeatedly abused as high-value entry points into enterprise environments. Threat actors moved past individual virtual machines. The hypervisor and management layer became the real target. Zero-days and privilege escalation flaws were actively abused, often supporting long-term access.

Once VMware was compromised, attackers gained durable, hard-to-see access with room to expand laterally and persist for months. These incidents reinforced how central VMware infrastructure has become to modern operations, and how damaging a failure at that layer can be.

Key VMware Vulnerabilities Exploited and Observed in 2025

- CVE-2025-22224, CVSS 9.3 (VCMI Heap Overflow) - A local attacker with administrative access to a virtual machine could exploit a heap overflow in the VMCI component to execute code as the VMX process on the host, creating a direct path toward hypervisor-level compromise.

- CVE-2025-22225, CVSS 8.2 (ESXi Arbitrary Kernel Write) - This flaw allowed attackers operating inside the VMX process to perform arbitrary kernel writes on ESXi, effectively escaping the virtual machine sandbox and gaining control over the underlying host system.

- CVE-2025-22226, CVSS 7.1 (HGFS Information Disclosure) - An information disclosure issue in VMware's Host-Guest File System exposed memory from the VMX process, giving attackers with elevated access insight into sensitive host-level data that could support follow-on exploitation.

- CVE-2025-41244, CVSS 7.8 (VMware Tools Local Privilege Escalation) - A local user with limited rights on a guest VM could escalate privileges to root when VMware Tools was in use and managed through Aria Operations, opening the door to full system control and lateral movement across the virtual environment. Broadcom confirmed this flaw may have been exploited in real-world attacks.

- CVE-2025-41245, CVSS 4.9 (Aria Operations Information Disclosure) - This vulnerability exposed credentials and sensitive data to authenticated users within Aria Operations, increasing the risk of account takeover and unauthorized access to other managed systems.

- CVE-2025-41246, CVSS 7.6 (VMware Tools Improper Authorization) - Improper access controls in VMware Tools for Windows allowed attackers with valid credentials to access other guest virtual machines, weakening isolation between workloads and increasing lateral movement risk.

- Exploitation of VMware vCenter and ESXi by BrickStorm Operators - Chinese state-linked actors abused weaknesses in VMware vSphere environments to deploy the BrickStorm backdoor, create rogue virtual machines, harvest snapshots, and quietly expand into identity systems and cloud services. While not tied to a single CVE, the activity proved how exposed or poorly segmented VMware management layers could be turned into long-term espionage platforms.

Palo Alto

Not every major security incident in 2025 came from a major zero-day. Some of the most impactful issues were quieter and within trusted tools and integrations that organizations rarely question.

This year reinforced a hard truth and that truth is that attackers don't always take the obvious route. Sometimes they walk in through software you already trust, using valid access paths that never trigger a firewall rule.

Palo Alto Networks – Salesloft Drift OAuth Token Abuse (Supply Chain Incident)

- Attackers abused stolen OAuth tokens from the Salesloft Drift integration to access Palo Alto Networks' Salesforce environment, bypassing traditional authentication controls entirely.
- The intrusion allowed access to customer contact data, internal sales records, and support case information, which was then scanned for credentials, cloud access keys, and VPN or SSO secrets using automated tooling.
- While Palo Alto confirmed that products, firewalls, and customer-deployed systems were not impacted, the incident showed us how SaaS integrations and API tokens can become high-value attack paths when compromised.
- This breach was part of a broader supply chain campaign tracked by Google as UNC6395, affecting hundreds of organizations and reinforcing the risk tied to OAuth trust relationships and CRM platforms as lateral-movement launch points.

Fortinet

Fortinet had a busy year, and not in a good way. Across 2025, multiple Fortinet products were hit with actively exploited zero-days, while older firewall flaws continued to fuel ransomware campaigns long after patches were available.

Internet-facing management interfaces, SSL VPNs, and overlooked appliances like voice and monitoring systems kept showing up in attack chains. For defenders, 2025 reinforced that Fortinet environments need tighter patch discipline and closer attention beyond just the firewall.

Fortinet Vulnerabilities Exploited in 2025

- CVE-2025-32756, CVSS 9.8 (FortiVoice Stack-Based Buffer Overflow) - A stack-based buffer overflow in FortiVoice and several related Fortinet products allowed unauthenticated attackers to execute arbitrary code via crafted HTTP requests. Active exploitation involved malware deployment, credential harvesting, log deletion, and network scanning, with FortiVoice systems directly targeted.

- CVE-2025-58034, CVSS 6.7 (FortiWeb OS Command Injection) - An authenticated command injection flaw in FortiWeb allowed attackers to execute OS-level commands using crafted HTTP requests or CLI input. Exploitation was observed in the wild shortly after disclosure, confirming active abuse of administrative access paths on web application firewalls.

- CVE-2024-21762, CVSS 9.8 (FortiGate SSL VPN Remote Code Execution) - A remote code execution vulnerability in FortiOS and FortiProxy SSL VPN functionality allowed unauthenticated attackers to compromise internet-facing FortiGate devices. Even in patched environments, leftover symlinks were later abused for persistence and follow-on access.

- CVE-2024-21762 and CVE-2024-55591, CVSS 9.8 (Qilin Ransomware Exploitation of Unpatched Fortinet Firewalls) - Qilin ransomware operators actively exploited CVE-2024-21762 and CVE-2024-55591 to compromise unpatched FortiGate devices. These vulnerabilities were used for initial access, persistence, and ransomware deployment.

- FileFix Fortinet-Themed Cache Smuggling Campaign - A Fortinet-branded social engineering campaign used cache smuggling and hidden PowerShell execution to deliver malware without visible downloads. While not a Fortinet product vulnerability, the technique abused trusted Fortinet branding and bypassed common endpoint detection controls.

Microsoft

Microsoft's biggest problems in 2025 were everyday Windows components getting abused over and over again. Attackers focused on kernel drivers, logging systems, and scripting engines that sit close to the operating system's core.

Once they got a foot in the door, these flaws made it easy to take full control of a system, shut off security tools, and move around without much resistance. The vulnerabilities below stood out this year because they were actively exploited, easy to chain together, and showed up again and again in attacks.

Microsoft Vulnerabilities Exploited in 2025

- CVE-2025-62215, CVSS 7.8 (Windows Kernel Elevation of Privilege) - A race condition and improper memory handling issue in the Windows Kernel allowed a local attacker with low privileges to corrupt kernel memory and gain SYSTEM-level access. While it did not provide initial access, it reliably turned any existing foothold into full control of the system, giving attackers the ability to disable security tools, dump credentials, and establish persistence. This vulnerability was

confirmed exploited in the wild and impacted both Windows 11 and Windows Server systems.

- CVE-2025-30400, CVSS 7.8 (DWM Core Library Elevation of Privilege) - A use-after-free vulnerability in the Desktop Window Manager (DWM) Core Library allowed attackers to escalate privileges to SYSTEM once code execution was already present. Because DWM is a core Windows component, exploitation provided a direct and reliable path to full system control and was actively abused alongside other Windows zero-days.

- CVE-2025-32701, CVSS 7.8 (Windows Common Log File System Driver Elevation of Privilege) - This use-after-free flaw in the Common Log File System (CLFS) driver allowed attackers to gain SYSTEM privileges after initial compromise. CLFS vulnerabilities appeared repeatedly throughout 2025 and became a familiar tool for attackers seeking fast privilege escalation inside Windows environments.

- CVE-2025-32706, CVSS 7.8 (Windows Common Log File System Driver Elevation of Privilege) - An improper input validation issue affecting the CLFS driver enabled local privilege escalation to SYSTEM. Like other CLFS flaws patched in 2025, this vulnerability reinforced a broader trend of attackers abusing Windows logging and kernel-adjacent components to move up the privilege ladder quickly.

- CVE-2025-32709, CVSS 7.8 (Ancillary Function Driver for WinSock Elevation of Privilege) - A use-after-free vulnerability in the afd.sys driver allowed attackers to escalate privileges locally to SYSTEM. This driver has appeared in multiple exploited vulnerabilities over recent years, and its continued abuse in 2025 showed attackers' preference for stable, well-understood paths to kernel-level access.

- CVE-2025-30397, CVSS 7.5 (Microsoft Scripting Engine Remote Code Execution) - A type confusion flaw in Microsoft's Scripting Engine allowed remote code execution through malicious web content rendered in Edge or Internet Explorer mode. While this vulnerability required user interaction, successful exploitation gave attackers a clean entry point that could then be paired with elevation-of-privilege bugs to fully compromise a system.

Looking back on 2025, the most damaging activity came from attackers going after the systems organizations rely on to run their business. Network gear, virtualization

platforms, identity-connected tools, and core Windows components kept showing up because they offered the fastest path to control. When those layers failed, attackers sat and waited.

Top Threat Actors of 2025

The threat actors that defined 2025 did not succeed because of new tactics and techniques. They succeeded because they refined the ones that already worked. These groups leaned hard into credential theft, social engineering, trusted service abuse, and data extortion, then ran those tactics at scale with discipline.

As some ransomware operations shut down or fractured, affiliates quickly shifted to groups that were already stable and profitable, driving sharp increases in activity. Manufacturing, healthcare, financial services, government, retail, and technology organizations took the brunt of the impact. Identity and cloud-heavy environments were frequent targets. These groups mattered because their activity was consistent.

Medusa

Medusa continued to gain momentum in 2025 by operating less like a traditional ransomware operation and more like a coordinated extortion business. The group focused on data theft, public pressure, and repeat targeting, often returning to victims even after payment.

Rather than relying on new exploits, Medusa capitalized on known flaws in widely deployed remote-access and file-transfer tools, paired with aggressive use of leak sites and social media to force action. Healthcare, education, government, and manufacturing organizations remained their primary targets, where downtime and public exposure carried immediate consequences.

- TTPs – Initial access via ScreenConnect, Fortinet EMS, GoAnywhere flaws, credential abuse, lateral movement with PsExec and RMM tools, data theft before encryption, ESXi targeting, triple extortion
- Tools – AnyDesk, PDQDeploy, SimpleHelp, MeshAgent, Rclone, PowerShell, PsExec, Mimikatz
- Country of Origin – Russia-aligned (Russian-language infrastructure, CIS avoidance)
- Most Targeted Industries – **Healthcare**, **education**, **government** and municipal services, **manufacturing**, legal and professional services

- Most Targeted Countries – United States, Canada, United Kingdom, France, Australia, Philippines
- Companies Breached (Year/Month) – Minneapolis Public Schools (02/2023), Toyota Financial Services (11/2023), Henry County IL (03/2024), Monmouth College (12/2023), Tarrant County Appraisal District TX (04/2024), multiple healthcare and education orgs (09/2025)
- Ransom Demands – $100K–$15M typical, up to $50M (Synnovis, 2024)
- Victim Count – 300+ confirmed victims globally

Qilin

Qilin emerged as the most active ransomware operation of 2025 by taking on displaced affiliates and scaling an already mature ransomware-as-a-service model. Following the shutdown of competing groups, Qilin's activity surged, with attacks spanning **government**, **healthcare**, **education**, **manufacturing**, and **financial services**.

The group combined data theft, encryption, and sustained pressure through leak sites and secondary channels, while increasingly targeting ESXi environments and cloud-connected infrastructure.

- TTPs – Phishing, VPN and edge device exploitation, credential dumping, RDP and RMM abuse, ESXi encryption, double extortion, cloud data theft (Snowflake, SFTP)
- Tools – Mimikatz, DonPAPI, PsExec, PowerShell, Cobalt Strike, RMM agents, ChaCha20, AES-256, RSA-4096
- Country of Origin – Russia (Russian-language forums, CIS avoidance)
- Most Targeted Industries – **Manufacturing**, **healthcare**, **government**, **education**, **financial services**, **retail**
- Most Targeted Countries – United States, France, Canada, South Korea, Spain, Japan
- Companies Breached (Year/Month) – Synnovis UK (06/2024), The Big Issue UK (03/2024), Asahi Group Holdings JP (09/2025), Alu Perpignan FR (09/2025), MedImpact US (10/2025), Cleveland Municipal Court US (02/2025), Shamir Medical Center IL (2025)
- Ransom Demands – $300K–$10M reported in 2025, $50M demanded in 2024 (Synnovis)
- Victim Count – 701 claimed in 2025, 118 confirmed; 926 claimed total since 2022

Scattered Spider

Scattered Spider was one of the most disruptive non-traditional ransomware threat actors in 2025. The operation focused on identity compromise rather than malware delivery. The group relied on layered social engineering, helpdesk manipulation, and SSO abuse to take over privileged accounts, often without deploying ransomware at all.

Financial services, retail, airlines, **technology firms**, and SaaS-heavy organizations were frequent targets. When encryption did occur, it was often secondary to data theft and delayed extortion.

- TTPs – Vishing and helpdesk impersonation, MFA fatigue, SIM swapping, SSO token takeover, identity persistence, cloud abuse, ESXi encryption in later stages
- Tools – AnyDesk, ScreenConnect, Splashtop, Tactical RMM, Ngrok, Teleport, Mimikatz, Raccoon Stealer, DragonForce ransomware
- Country of Origin – English-speaking actors, likely Western-based, exact location unknown
- Most Targeted Industries – **Financial services**, **retail**, airlines, technology, luxury brands, SaaS providers
- Most Targeted Countries – United States, United Kingdom, France, Australia, Canada
- Companies Breached (Year/Month) – Marks & Spencer (2025), Adidas (2025), Victoria's Secret (2025), Jaguar Land Rover (2025), Kering Group (2025), unnamed US bank (post-retirement claim, 2025)
- Ransom Demands – Variable, often delayed extortion following data theft
- Victim Count – Dozens of confirmed large enterprise victims since late 2024

Akira Ransomware

In 2025, Akira put its energy into targeting virtualized infrastructure and mid-sized organizations. After establishing itself in earlier years, the group refined its ESXi operations and used double extortion to increase pressure on victims with limited recovery options. Akira's operations favored speed and disruption, with attacks frequently tied to unpatched infrastructure and weak credential hygiene.

- TTPs – Phishing, RDP brute force, ESXi exploitation, credential theft, lateral movement, data theft followed by encryption
- Tools – Mimikatz, LaZagne, WinSCP, Rclone, AnyDesk, RustDesk, ChaCha20, RSA
- Country of Origin – Likely Russia-based or Russia-aligned
- Most Targeted Industries – **Manufacturing**, **finance**, **education**, IT services, **healthcare**
- Most Targeted Countries – United States, Canada, United Kingdom, Germany

- Companies Breached (Year/Month) – 4LEAF (2023), Park-Rite (2023), Family Day Care Services CA (2023), BridgeValley Community & Technical College WV (04/2023), multiple global victims (2024–2025)
- Ransom Demands – $50K–$500K typical
- Victim Count – 350+ global victims

Play

Play ransomware was a steady and disruptive force in 2025 by relying on volume and aggressive follow-through. The group continued to operate as a closed operation, favoring double extortion campaigns where data theft preceded encryption and negotiations were handled directly through one-to-one communication with victims.

Play's activity stayed concentrated around known weaknesses in perimeter systems, remote access tooling, and unpatched infrastructure, with ESXi environments increasingly targeted for maximum operational disruption. By mid-2025, law enforcement tracking placed Play among the most active ransomware groups of the year.

- TTPs – Exploitation of public-facing applications, abuse of valid credentials purchased from brokers, RDP and VPN access, Active Directory enumeration, credential dumping, lateral movement with PsExec, Group Policy abuse, data exfiltration prior to encryption, ESXi hypervisor targeting, double extortion with follow-up phone pressure
- Tools – AdFind, BloodHound, Grixba, Mimikatz, PsExec, PowerShell, WinPEAS, Cobalt Strike, SystemBC, WinRAR, WinSCP, GMER, IOBit, PowerTool, SimpleHelp (abused), custom Play ransomware binaries
- Country of Origin – Likely Russia-aligned (German email infrastructure, CIS avoidance patterns, Russian-language tradecraft indicators)
- Most Targeted Industries – **Government** and municipal services, **healthcare**, **education**, **manufacturing**, critical infrastructure, IT service providers
- Most Targeted Countries – United States, Canada, Germany, Switzerland, Australia, countries across Western Europe and Latin America
- Companies Breached (Year/Month) – Oakland CA (2023), Lowell MA (2023), Dallas County TX (2023), Swiss government IT provider (2023), Microchip Technology US (2024), multiple U.S. public sector entities tied to SimpleHelp exposure (01–05/2025)
- Ransom Demands – Not disclosed in initial notes; negotiated directly via unique @gmx.de or @web[.]de email addresses, often reinforced with phone calls threatening data release
- Victim Count – ~900 affected entities globally as of May 2025, with continued activity observed into mid-2025

Cl0p

CL0P stood out in 2025 not because of constant activity, but because of impact. The group continued to prove that a single, well-timed supply-chain exploit can outweigh months of traditional ransomware operations. Rather than broad spray-and-pray campaigns, CL0P focused on exploiting zero-day vulnerabilities in widely trusted enterprise software, allowing it to compromise hundreds or thousands of organizations in short bursts.

By 2025, the group had largely shifted away from widespread encryption toward data-only extortion, relying on mass theft and pressure to receive payment while limiting operational noise.

- TTPs – Exploit of zero-day and high-severity vulnerabilities in managed file transfer platforms, web shell deployment (LEMURLOOT, DEWMODE), database enumeration, targeted data exfiltration without lateral movement, delayed executive-level extortion emails, selective data disclosure on leak sites
- Tools – LEMURLOOT web shell, DEWMODE web shell, Truebot downloader, FlawedGrace RAT, SDBot, Cobalt Strike, PowerShell, custom SQL queries against MFT backends
- Country of Origin – Russia-aligned (TA505 lineage, Russian-language tradecraft, CIS victim avoidance)
- Most Targeted Industries – **Manufacturing**, professional services, **financial services**, **government**, **healthcare**, **education**, **retail**
- Most Targeted Countries – United States, United Kingdom, Germany, France, Canada, Netherlands
- Companies Breached (Year/Month) – Maastricht University NL (12/2019), Jones Day US (01/2020), Kroger US (01/2020), City of Toronto CA (01/2023), Rubrik (01/2023), BBC UK (06/2023), Johns Hopkins University US (06/2023), Ernst & Young (06/2023), Zellis UK (06/2023), multiple Oracle E-Business Suite customers (09/2025)
- Ransom Demands – Variable and often undisclosed; typically negotiated directly via executive outreach rather than posted demands
- Victim Count – Estimated 3,000+ U.S. organizations and 8,000+ globally tied to MOVEit alone; hundreds more across Accellion, GoAnywhere, Cleo, and follow-on campaigns

These threat actors show how ransomware and extortion in 2025 became less about innovation and more about execution. The most successful groups went after identity systems and trusted services. They targeted software organizations rely on every day. These attacks applied pressure where recovery took the longest and visibility was limited. These groups reuse the same access paths. Ransomware, data theft, and identity compromise often overlap.

ASPIRE'S PREDICTIONS FOR 2026

In 2025, threat actors kept using the same access paths because they worked. Identity systems and exposed infrastructure remained easy targets. Rather than chasing new techniques, attackers continued to refine and scale the same methods that proved reliable across ransomware, extortion, and espionage campaigns. Here are some of Aspire's predictions for the year ahead:

- Continued exploitation of edge devices and exposed infrastructure – VPNs, firewalls, and internet-facing management interfaces will remain primary entry points, particularly in Fortinet, Cisco, and similar network environments where patching delays and configuration drift persist.

- Continued focus on ESXi and virtualized environments – Ransomware groups such as Qilin, Play, and Akira are expected to continue targeting VMware infrastructure to maximize operational disruption and limit recovery options, especially in mid-sized enterprises.

- Expansion of identity-based intrusions – Social engineering, helpdesk impersonation, MFA fatigue, and SSO abuse will continue to be used. Scattered Spider relied on these methods throughout 2025. Full environment compromise without malware will continue to be viable where identity controls and verification processes are weak.

- Ongoing abuse of SaaS integrations and OAuth trust paths – API tokens, CRM integrations, and cloud service connections will remain attractive targets for data theft and lateral movement, building on supply-chain activity observed in 2025.

- Ransomware operations prioritizing data theft over encryption – Encryption will not disappear. Extortion will increasingly rely on stolen data and follow-up pressure rather than immediate disruption.

- Affiliate consolidation around stable ransomware brands – Groups like Qilin and Play already have stable infrastructure. Affiliates tend to move toward groups that pay reliably. That keeps attack volume high without changing how these groups operate.

- Persistent exploitation of known vulnerabilities – Older, well-documented flaws will continue to be exploited. Many systems remain exposed. Patch gaps and limited visibility will matter more than new zero-days.

The activity seen in 2025 will continue into 2026. Attackers rely on exposed infrastructure and identity systems because those paths remain effective. Without changes at those layers, the tactics stay the same.

***Please Note**: These predictions are based on Aspire's CTI content and public reporting from several established sources such as Fortinet, Cisco, Broadcom, government agencies, and public incident disclosures.*

Conclusion

The defining lesson of 2025 was not that attackers became more sophisticated, it was that they became more focused. The most damaging incidents consistently stemmed from the compromise of systems organizations depend on to manage everything - network infrastructure, virtualization platforms, identity services, and trusted SaaS integrations. When those layers failed, attackers gained control that was difficult to detect and often discovered only after data theft or extortion pressure began.

Threat actors succeeded by reusing what already worked. Ransomware groups grew by reusing access paths and adding affiliates. They did not need to innovate. Identity-based attacks worked because trust was easy to manipulate. Supply-chain incidents worked because of timing and reach. Across these campaigns, visibility gaps were the common problem.

As organizations move into 2026, the risk is not a sudden shift in attacker behavior, but familiarity. The same vulnerabilities, misconfigurations, and trust relationships that were abused throughout 2025 are still present across many environments today. Without attention to identity controls, exposed infrastructure, virtualization security, and third-party integrations, attackers will not need to change tactics to launch successful attacks. They already know where the gaps are.

ASPIRE PROTECTS

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors. Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyberattacks.
- **Aspire Managed Detection and Response (MDR)**
  - Accelerate the maturity of your security operations and reduce risk with faster threat detection and response capabilities. Aspire MDR delivers around-the-clock protection across cloud, network, and endpoints in one integrated solution.
  - Our team of experts act as an extension of your IT operations to quickly identify and mitigate security threats before they impact your business.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

SUPPORTING DOCUMENTATION

ClickFix Gets Creative: Malware Buried in Images | Huntress

ClickFix: An Adaptive Social Engineering Technique

Think before you Click(Fix): Analyzing the ClickFix social engineering technique | Microsoft Security Blog

Oracle EBS Victims Include Korean Air, University Of Phoenix

Uncover your compromised credentials from the deep and dark web - Cyberint

Dartmouth College Oracle EBS Data Breach: 1,494+ Affected in Zero-Day Hack

Phoenix University data breach exposes 3.4MPhoenix University data breach exposes another 3.4M victims of Cl0p Oracle hacks | Cybernews

Cl0p Is Back, Exploiting Supply Chains Again. by Lucie Cardiet

Cyble report shows manufacturing hit hard as zero-day exploits, illicit access sales reshape threat landscape - Industrial Cyber

#StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability | CISA

#StopRansomware: Akira Ransomware

Play Ransomware: Analysis, Detection, and Mitigation

US aerospace and defence manufacturer breached, hackers claim | Cybernews

Anchor Industries Evansville cyber attack under investigation

FBI: Play ransomware gang has attacked 600 organizations since 2023 | The Record from Recorded Future News

#StopRansomware: Play Ransomware | CISA

LG battery subsidiary says ransomware attack targeted overseas facility | The Record from Recorded Future News

FBI calls Akira ‘top five’ ransomware variant out of 130 targeting US businesses | CyberScoop

Anatomy of an Akira Ransomware Attack: When a Fake CAPTCHA Led to 42 Days of Compromise

Akira group has defrauded $244 million in ransomware payments, says FBI | SC Media

Ransomware hits LG Energy Solution’s overseas facility | SC Media

Old SonicWall vulnerability resurfaces in Akira ransomware campaign, Darktrace warns - Industrial Cyber

Akira ransomware's evolving tactics prompt global agencies to strengthen critical infrastructure guidance - Industrial Cyber

UK Healthcare provider HCRG battles Medusa ransomware threat

SimonMed Imaging discloses a data breach impacting over 1.2 million people

#StopRansomware: Medusa Ransomware | CISA

Qilin claims pharmacy benefit manager MedImpact | Cybernews

Qilin ransomware escalates rapidly in 2025, targeting critical sectors with 700 attacks amid RansomHub shutdown - Industrial Cyber

Scattered Spider Targets Financial Sector After Alleged Retirement | Security Magazine

Feds Tie 'Scattered Spider' Duo to $115M in Ransoms – Krebs on Security

Scattered Spider | CISA

Appendix II: Disclaimer

This document and its contents are not intended to serve as legal advice and should not be used as a substitute for it. The results of a Security Risk Assessment are intended to guide the implementation of diligent measures to reduce the risk of potential vulnerabilities being exploited to compromise data.

While the Services and this report may offer information that the Client can use to support its compliance efforts, the responsibility for evaluating and fulfilling compliance obligations rests solely with the Client, not Aspire. This report does not guarantee or assure the Client's compliance with any law, regulation, or standard.