halcyon

2025 Ransomware Evolution Report

Table of Contents

halcyon

Ransomware Landscape: 2025 Overview

Throughout 2025, ransomware gangs increased the speed and scale of their operations. Ransomware continued to grow as a durable, industrialized ecosystem built on specialization, shared infrastructure, and rapid regeneration rather than any single brand. Law enforcement pressure and infrastructure seizures disrupted major operations, driving fragmentation, rebranding, and intensified competition across a more fluid landscape.

In many incidents, Halcyon blocked ransomware operations after other controls had failed, underscoring persistent gaps at access and identity layers. The line between financially motivated and state-aligned activity continued to blur, complicating attribution and response. The lesson for 2026 is clear: ransomware is not just malware, but an access-driven, identity-centric intrusion model operating at speed and scale, requiring resilience, coordinated response, and sustained pressure on attacker access paths alongside prevention.

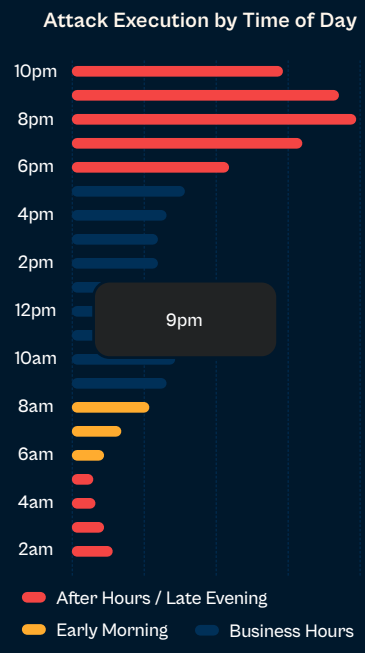
The trends below distill the most significant patterns observed across the year's activity and impact, informed by Halcyon analysis of ransomware prevention, thousands of blocked ransomware execution attempts, and incident response observations spanning hundreds of distinct variants.

Top 2025 Trends

- **Dwell Time Compression and Rapid Intrusion Execution:** Ransomware operations were significantly faster compared with 2024. Dwell time continued to compress through 2025, with intrusion timelines collapsing from days to hours in the fastest-moving cases, leaving little to no effective response window once access was established. With groups such as Akira and Play, initial access progressed to encryption attempts often in a single night. A key driver of this acceleration is the growing focus on hypervisor and virtualization platforms, including ESXi- and Hyper-V–based environments, where a single compromise enables rapid, simultaneous impact across large numbers of virtualized workloads.
- **Attack Timing Aligned to Reduced Defensive Coverage:** Ransomware gangs continued to attack when targeted entities' security teams were less likely to respond, with 69 percent of observed attack attempts occurring outside business hours. Temporal analysis shows attackers deliberately timing operations for nights and weekends due to limited monitoring; late evening was the most common execution window.

69%

of attacks execute outside business hours



halcyon

- **Defense and Security Bypass Became Standard:** Most attempted attacks observed in 2025 deliberately sought to evade or impair organizations' defensive and security tooling, including Endpoint Detection and Response (EDR). These ransomware attempts most occurred after endpoint controls were bypassed or degraded, with tens of thousands of EDR bypass and suppression events detected over the year.
- **Expansion of Bring Your Own Vulnerable Driver (BYOVD) and Kernel-Level Defense Evasion:** Detections further shows continued expansion of BYOVD abuse as a post-compromise technique to achieve kernel-level control and bypass endpoint detection and response mechanisms. Signed but vulnerable drivers were leveraged to escalate privileges, disable or impair EDR and other endpoint protections, and operate below user-mode visibility, increasing attacker ability to undermine endpoint integrity and evade detection.
- **Disproportionate Impact on Small and Mid-Sized Organizations (SMB):** Small and mid-sized organizations faced a disproportionate share of ransomware risk throughout 2025, driven primarily by access economics and resource constraints. Halcyon data shows ransomware gangs targeted SMBs at nearly four times the rate of large organizations. Observations reflect a high concentration of ransomware activity targeting SMBs where dedicated security staffing is limited, security responsibilities are often combined with general IT functions, and visibility is uneven across identity, remote access, and endpoint activity. These characteristics make SMB environments more accessible and less resilient to sustained intrusion activity.
- **Repeated Targeting of IT/OT and Critical Service Environments:** Information Technology (IT)/Operational Technology (OT)-adjacent environments remained high-value ransomware targets due to structural constraints that amplify the impact of disruption once access is obtained. Organizations operating manufacturing processes, industrial systems, and critical infrastructure often rely on tightly coupled IT and OT environments where compromise of identity, remote access, or management systems can cascade rapidly into operational outages. In these settings, downtime pressure escalates quickly due to safety considerations, regulatory obligations, and service continuity requirements, increasing attacker leverage and payment pressure. Halcyon detections across 2025 reflect repeated targeting of such environments, including follow-on attempts after initial incidents, reinforcing attacker preference for organizations where recovery paths are constrained, restoration timelines are extended, and disruption carries immediate operational and societal consequences.

As ransomware dwell time collapsed from days to hours, attackers gained an overwhelming operational advantage that traditional detection and response cycles were never designed to address.

State and Criminal Activity Blur: In 2025, we saw continued overlap between nation state and criminal ransomware campaigns. Cybercriminal tactics offer nation-state actors several advantages. They are fast, scalable, and highly repeatable. They exploit common weaknesses in remote access, identity systems, and virtualization platforms that exist across nearly every critical environment. And critically, they complicate attribution, allowing attackers to operate below traditional response thresholds. Russia, Iran, China, and North Korea have directly conducted or been tied to ransomware attacks. In many of these campaigns, ransomware functions less as a monetization tool and more as a delivery mechanism for obfuscation or disruption. One of the year's strongest examples was the Warlock ransomware campaign that rapidly followed China's espionage campaign against on-premises SharePoint servers.

Shift From Group Branding to Access-Driven Ransomware Ecosystems: In 2025, ransomware gangs continued to fragment, rebrand, and operate in smaller, less stable configurations following successful law enforcement takedowns and infrastructure disruptions that degraded major ransomware operations. Throughout the year, Halcyon observed more than 70 new gangs emerge as well as increasingly inconsistent leak-site behavior across campaigns. These conditions complicate attribution as affiliates bring similar tactics to new groups, and it becomes increasingly difficult to initially determine the validity of new groups' claims.

Nation-state actors have embraced ransomware as the perfect proxy because it is fast, scalable, and provides plausible deniability that shields governments from direct attribution and accountability.

Top Ransomware Groups 2025

The most prominent ransomware groups in 2025 demonstrated both the scale and competitive churn of the modern Ransomware-as-a-Service (RaaS) and data extortion criminal ecosystem. High attack volume remained closely correlated with mature affiliate programs, reliable extortion infrastructure, and consistent leak-site operations. Telemetry from 2025 reflects this concentration, with a relatively small number of operators accounting for a disproportionate share of blocked ransomware activity, even as hundreds of distinct variants circulated across the ecosystem. Over the year, thousands of ransomware actions tied to this top tier of operators were prevented, including encryption attempts stopped on protected devices as well as earlier access, lateral movement, and tooling behaviors, underscoring how scale is driven by execution discipline and operational maturity rather than sheer family proliferation.

ESTABLISHED LEADERS

Top Groups and Ones to Watch in 2026

Qilin

Telemetry Degradation

Degrades endpoint visibility and logging before payload launch; alerts that should fire during encryption may not; defenders respond to an incomplete picture.

Akira

Hypervisor Targeting

Hypervisor-first; one credential compromise encrypts entire virtual estate simultaneously; single-night intrusion-to-encryption sequences observed.

ClOP

Encryption-Free Extortion

No encryptor deployed; pure mass data theft against MOVEit, GoAnywhere and Oracle EBS; no decryption key exists; payment buys only a deletion promise.

Play

Per-Deploy Recompilation

Encryptor recompiled per deployment; no two attacks share a binary; signature detection defeated by design; requires behavioral analytics to catch.

SafePay

Closed Operator Model

Closed non-affiliate model, domain admin validate before every launch, eliminates variability that typically makes RaaS groups trackable.

Qilin

- **Business Model:** Script-driven RaaS with accelerated tempo and centralized control
- **Access and Execution Tradecraft:** Compromised credentials against exposed Remote Desktop Protocol (RDP), Virtual Private Networks (VPN), and admin services; rapid lateral movement via PsExec and WMI; limited reconnaissance; pre-encryption visibility suppression
- **Exfiltration and Encryption:** Local staging and SFTP exfiltration via Cyberduck; rapid SMB encryption using Windows and Linux encryptors; deterministic sequencing and consistent leak-site cadence
- **Industry Targeting:** Manufacturing and industrial networks globally

Akira

- **Business Model:** Perimeter-first exploitation with deterministic execution
- **Access and Execution Tradecraft:** Exploited exposed VPN and management interfaces; persistent AnyDesk access; automated discovery of network file shares and mapping of Active Directory (AD) relationships to identify privileged accounts and efficient lateral movement paths; Impacket-based lateral movement; endpoint suppression prior to encryption
- **Exfiltration and Encryption:** Near-simultaneous Windows, Linux, and ESXi encryption; hypervisor prioritization; backup disablement; double extortion
- **Industry Targeting:** Manufacturing, healthcare, education, and the public sector; concentrated in North America and Europe

ClOp

- **Business Model:** Exploitation-driven data theft model tied to vulnerability disclosure cycles
- **Access and Execution Tradecraft:** MOVEit, GoAnywhere, Gladinet, and Oracle EBS exploitation for unauthenticated access and session harvesting; minimal dwell; negligible lateral movement; automated extraction
- **Exfiltration and Encryption:** Bulk scripted data exfiltration; no encryptor deployment; aggressive leak-site disclosures after mass compromise events
- **Industry Targeting:** Cross-industry, global; victim selected based on exposure

The most prolific ransomware operators in 2025 were distinguished not by technical sophistication but by operational maturity, affiliate discipline, and the reliability of their extortion infrastructure.

Play

- **Business Model:** Centralized exploit-led model emphasizing execution control over affiliate scale
- **Access and Execution Tradecraft:** Exposed perimeter and remote management exploitation; Grixba discovery; SystemBC tunneling; PsExec and GPO propagation; limited interactive activity
- **Exfiltration and Encryption:** Custom intermittent encryption with per-deployment recompilation; rapid, reliable multi-host execution
- **Industry Targeting:** Manufacturing, healthcare, logistics; primarily North America and Europe

SafePay

- **Business Model:** Closed non-affiliate model with fixed deterministic runbook
- **Access and Execution Tradecraft:** alidated domain admin access; SMB share enumeration; PsExec and scheduled task lateral execution; minimal operator interaction
- **Exfiltration and Encryption:** Simultaneous encryption of multiple Windows machines; high reliability; routine leak publication
- **Industry Targeting:** Small and mid-sized organizations across industries; North America and Europe

A small number of ransomware operators accounted for a disproportionate share of global attack volume, proving that scale in this ecosystem is driven by execution consistency rather than sheer numbers.

Ransomware Groups Gaining Traction in 2025

The top five groups to watch in 2026 either emerged or materially accelerated during 2025, demonstrating momentum through sustained posting cadence, expanded reach, or increased organizational maturity. Their trajectories suggest an ecosystem where new brands can scale quickly through aggressive extortion models, rapid infrastructure stand-up, and flexible operating structures that range from small, closed teams to early-stage affiliate programs, even as long-term durability and technical depth remain uneven.

Below are the top five ransomware groups gaining traction and their operating models.

RISING THREATS

Top Groups and Ones to Watch in 2026

DragonForce

Cartel-Style RaaS Group

Cartel-style affiliate infrastructure; adaptive payload logic, standardized playbooks lower skill floor and expand the effective operator pool.

Sinobi

Session Token Hijacking

Steals authenticated VPN session tokens not credentials; MFA rendered completely ineffective; token theft persists through post-incident credential rotation.

Sarcoma

Persistent Tor Infrastructure

Tor negotiation portals and onion leak sites remain live throughout campaigns; extortion pressure continues regardless of victim containment actions.

NightSpire

Fortinet Specialization

Built exlusively around FortiOS and FortiProxi authentication bypass; near-zero dwell time; any internet-facing Fortinet deployment is named specific risk.

DireWolf

Pre-Confirmed Admin Control

Closed non-affiliate model, domain admin validate before every launch, eliminates variability that typically makes RaaS groups trackable.

DragonForce

- **Business Model:** Affiliate-based selective RaaS with structured cartel-style infrastructure
- **Access and Execution Tradecraft:** Initial footholds via exploitation of Remote Monitoring and Management (RMM) tools, social engineering, and credential theft; SystemBC and Cobalt Strike persistence; automated network scanning and cross-platform payload delivery across Windows, Linux, and ESXi
- **Exfiltration and Encryption:** ChaCha8 encryption with selective logic; shadow copy deletion; coordinated multi-platform impact; standardized affiliate execution
- **Industry Targeting:** Manufacturing, logistics, healthcare; primarily North America and Europe

Sinobi

- **Business Model:** Fast, mid-market-focused RaaS with lineage-based tooling and repeatable execution pipeline
- **Access and Execution Tradecraft:** SonicWall SSL VPN session hijacking; RMM and AnyDesk abuse; MSP credential compromise; endpoint security disablement; LSASS dumping; lateral movement via RDP, SMB, and WMI; RClone exfiltration
- **Exfiltration and Encryption:** Curve25519 key exchange with AES-128-CTR encryption; multi-threaded Windows implementation; high-volume data theft preceding encryption
- **Industry Targeting:** Mid-market manufacturing, professional services, technology-adjacent sectors; North America and Western Europe

Sarcoma

- **Business Model:** Hybrid RaaS with selective affiliate recruitment and consistent campaign cadence
- **Access and Execution Tradecraft:** RMM-centric remote discovery and execution; consistent sequencing; exfiltration via RClone, WinSCP, and cURL with 7z compression
- **Exfiltration and Encryption:** Coordinated encryption across Windows, Linux, and ESXi; shadow copy deletion via vssadmin; persistent Tor negotiation portals and onion leak sites
- **Industry Targeting:** Manufacturing, technology, services; North America and Europe

Emerging ransomware groups demonstrated that a disciplined execution model and consistent operational tempo matter far more than technical sophistication or novel payloads.

NightSpire

- **Business Model:** Closed perimeter-first Fortinet exploitation model
- **Access and Execution Tradecraft:** FortiOS and FortiProxy authentication/session bypass; rapid credential harvesting and lateral movement via native Windows tools; minimal dwell and deterministic sequencing
- **Exfiltration and Encryption:** Coordinated environment-wide encryption; structured double extortion via persistent leak infrastructure
- **Industry Targeting:** Enterprises exposed via Fortinet deployments; North America and Europe

DireWolf

- **Business Model:** Closed non-affiliate model with centralized operator control and stable codebase
- **Access and Execution Tradecraft:** Confirmed administrative control prior to controlled lateral execution via native Windows services and remote process creation; minimal operational variation
- **Exfiltration and Encryption:** Static Golang encryptor; inline service termination and shadow copy deletion; coordinated batch encryption across reachable hosts
- **Industry Targeting:** Opportunistic cross-sector targeting; primarily North America and Europe

The most prolific emerging ransomware operators were not distinguished by novel payloads but by their ability to stand up reliable infrastructure, recruit selectively, and execute with consistency from the first campaign.

Attack Distribution

Geographic Distribution

Ransomware activity in 2025 remained heavily concentrated in North America and Western Europe, which together accounted for the majority of observed ransomware operations during the year. The United States alone represented over half of prevented ransomware activity. These regions also exhibited higher rates of after-hours execution and repeated intrusion attempts.

Industry Distribution

Ransomware gangs in 2025 targeted industries where downtime pressure, operational interdependence, and recovery constraints created strong extortion leverage. The most frequently targeted industry was manufacturing, accounting for roughly one-fifth of observed ransomware activity, followed by business services and construction.

While finance, energy, transportation, and retail represented a smaller share of total incidents, Halcyon assesses these industries are often selected for more targeted operations because service disruption can produce outsized economic impact, regulatory consequences, and downstream systemic effects disproportionate to attack volume. Attacks against healthcare targets demonstrated high impact, not only due to operational fragility and limited tolerance for downtime, but because service disruption directly elevates risk to patient life and safety. Education and transportation similarly showed disproportionate impact relative to frequency, where service availability is mission critical, and recovery windows are narrow.

RANSOMWARE TARGETING BY SECTOR

halcyon

Tactics, Techniques, and Procedures

Ransomware attackers in 2025 consistently prioritized access, identity control, and operational speed, leveraging trusted administrative tooling, a narrow set of high-impact perimeter vulnerabilities, and living-off-the-land (LotL) techniques to compress timelines and reduce detection. The following sections outline how these tools, tactics, and procedures favored reliability, reuse, and efficiency over innovation.

Attackers Prioritized Legitimate Remote Access Tools

During ransomware attempts in 2025, attackers consistently blended native operating system utilities, legitimate third-party software, and selectively deployed malicious tools as their operations progressed. Across ransomware intrusions Halcyon observed in 2025, initial access, lateral movement, and data exfiltration consistently exhibited the greatest diversity of tooling.

In particular, 78 percent of observed incidents involved attackers attempting to exploit legitimate remote monitoring and management (RMM) tools. Ransomware gangs view remote tools as low-friction access mechanisms because they are commonly pre-installed, broadly trusted, and capable of full remote administrative control.

Remote tool abuse was highly concentrated, with ConnectWise ScreenConnect, AnyDesk, and Splashtop accounting for 89 percent of observed RMM-related ransomware activity. Observed activity shows remote tooling used not only for initial hands-on-keyboard access, but also to maintain persistence, re-enter environments after credential harvesting, and accelerate lateral movement following automated enumeration. Even when remote tools were installed by attackers, their activity often went undetected.

ConnectWise ScreenConnect

- **Legitimate Uses:** Enterprise remote IT support and centralized administration for endpoints and servers, including troubleshooting, patching, configuration management, and incident response. Commonly deployed and trusted within standard enterprise access workflows.
- **Abusive Applications:** Persistent remote control after compromise; lateral movement and remote command execution without new tooling; coordinated ransomware deployment and data staging that blends into legitimate support traffic. Frequently used during after-hours windows for re-entry, multi-host execution, and pre-encryption data theft.
- **MITRE:** [T1219] [T1021.001] [T1569.002]

HALCYON, 2025

78%

of incidents abused legitimate RMM software

ConnectWise ScreenConnect	41%
AnyDesk	31%
Splashtop	17%
Other RMM	11%

halcyon

AnyDesk

- **Legitimate Uses:** Remote desktop access for IT support, remote work, and system administration across enterprise environments. Often internet-exposed or broadly permitted internally to enable interactive system management.
- **Abusive Applications:** Covert persistent access and hands-on-keyboard control for privilege escalation, defense evasion, lateral movement, and ransomware deployment. Frequently observed in after-hours activity, blending into normal administrative behavior and preceding coordinated multi-host encryption attempts.
- **MITRE:** [T1219] [T1021.001] [T1078]

Splashtop

- **Legitimate Uses:** Remote access and endpoint management for IT operations, remote workforce support, and centralized system administration. Widely deployed and trusted for interactive remote control across enterprise environments.
- **Abusive Applications:** Sustained remote access after credential compromise; lateral movement and remote execution across high-value systems; coordinated ransomware deployment while appearing as normal administrative activity. Commonly used during after-hours windows to maintain control and enable reliable multi-host encryption attempts.
- **MITRE:** [T1219] [T1021.001] [T1569.002]

Legitimate remote management tools are the preferred attack vector precisely because they are trusted, widely deployed, and indistinguishable from legitimate network traffic.

Vulnerability Exploitation

Ransomware operators in 2025 most commonly exploited vulnerabilities focused on a small number of perimeter technologies, including VPN appliances, remote management interfaces, and edge services that are broadly deployed and inconsistently patched. This concentration enabled fast intrusion timelines, repeatable execution, and simultaneous compromise across multiple environments sharing the same exposed services.

Ivanti Connect Secure

- **CVSS:** 9.0–10.0
- **Disclosure-to-Exploitation:** Pre-disclosure (weeks) to same day
- **Context:** Unauthenticated remote code execution (RCE) in internet-facing edge services was used for initial access and foothold establishment. This access vector underpins a significant share of ransomware executions blocked by Halcyon, particularly against VPN appliances, firewall platforms, and remote access gateways where exploitation required no user interaction.

Oracle E-Business Suite Remote Code Execution

- **CVSS:** 9.8
- **Disclosure-to-Exploitation:** Unknown (insufficient public timing fidelity)
- **Context:** Unauthenticated remote code execution (RCE) in internet-facing enterprise applications was used for initial access, session or account takeover, and follow-on data theft or extortion activity associated with ransomware operations. Halcyon observed this technique driving high-impact campaigns against widely deployed enterprise services, with exploitation frequently enabling direct access to sensitive data stores without requiring lateral movement or endpoint compromise.

Ransomware operators leverage a small set of widely deployed, inconsistently patched perimeter vulnerabilities because they are reliable, repeatable, and provide direct access to internal networks.

Fortinet FortiOS SSL VPN

- **CVSS:** 9.6
- **Disclosure-to-Exploitation:** < 1 week (often near immediate; sometimes suspected pre-patch)
- **Context:** Critical remote code execution (RCE) in internet-facing network security appliances was exploited for initial access, commonly followed by credential harvesting, lateral movement, and ransomware deployment. Halcyon observed this technique underpinning some of the fastest-moving ransomware intrusions during the year, particularly against VPN, firewall, and secure access appliances that provide direct connectivity into internal networks.

  In multiple blocked campaigns, exploitation of these appliances enabled attackers to bypass endpoint defenses entirely, harvest credentials at scale, and pivot laterally within hours, often culminating in coordinated, environment-wide encryption during a single after-hours window.

SonicWall SonicOS SSLVPN

- **CVSS:** 9.3
- **Disclosure-to-Exploitation:** Days to < 2 weeks (typically shortly after public PoC / advisory)
- **Context:** Widely exploited edge-device access control vulnerability in exposed SSL VPN services was used for initial access, including activity associated with Akira. SSL VPN vulnerability exploitation was one of the initial access vectors most consistently observed by Halcyon across blocked ransomware executions, particularly in mid-market and operationally constrained environments.

  In multiple cases observed by Halcyon, successful VPN exploitation enabled rapid acquisition of valid credentials and session context, allowing attackers to bypass MFA controls and move laterally without deploying endpoint malware. These intrusions frequently progressed overnight from access to attempted encryption.

The window between public vulnerability disclosure and active exploitation collapsed to hours, rendering traditional patch cycles functionally inadequate against the speed of modern ransomware intrusions.

Oracle E-Business Suite Server-Side Request Forgery (SSRF)

- **CVSS:** 9.1
- **Disclosure-to-Exploitation:** Unknown (insufficient public timing fidelity)
- **Context:** Server-side request forgery (SSRF) in enterprise applications was used for internal pivoting and access to sensitive resources, enabling follow-on compromise, lateral movement, and ransomware-related operations after initial access. Halcyon observed SSRF was often used as a control-plane pivot inside enterprise application stacks, enabling attackers to reach otherwise inaccessible internal services, harvest session material, and expand access without deploying additional tooling.

  This behavior aligns with exploitation-driven campaigns where compromise of an externally exposed application is rapidly converted into account takeover and automated data access, including activity documented by Halcyon involving ClOp abuse of Oracle E-Business Suite for account takeover and follow-on extortion workflows. (https://www.halcyon.ai/ransomware-research-reports/security-alert-clop-abuses-oracle-e-business-suite-for-account-takeover).

Zoho ManageEngine Suite flaws

- **CVSS:** 8.8–9.8
- **Disclosure-to-Exploitation:** Days to weeks (varies by CVE; often rapid after PoC/advisory)
- **Context:** Actively exploited vulnerabilities across multiple ManageEngine products were used for initial access. Halcyon found ManageEngine exploitation recurring as a perimeter-first entry point in ransomware intrusions, particularly where management interfaces were internet facing and operated with high privilege by design.

  In multiple blocked campaigns, initial access via ManageEngine services rapidly transitioned into credential harvesting, administrative access, and lateral movement using trusted tooling, enabling coordinated encryption attempts during the same after-hours operational window.

Perimeter vulnerabilities in VPN appliances, firewalls, and remote access services are not just entry points; they allow attackers to bypass endpoint defenses entirely and move directly into credential harvesting and lateral movement.

Windows CLFS

- **CVSS:** 7.8
- **Disclosure-to-Exploitation:** Pre-disclosure (zero-day)
- **Context:** Local privilege escalation, zero-day exploit post-initial access to obtain elevated privileges, disable security controls, and enable ransomware deployment. Halcyon observed local privilege escalation exploitation frequently occurring after perimeter access was established, enabling attackers to transition quickly from user or service-level access to full administrative control.

  Across blocked ransomware executions, local privilege escalation was closely associated with subsequent EDR and telemetry suppression, credential harvesting, and coordinated encryption attempts, reinforcing its role as a force multiplier that accelerates intrusion timelines and increases reliability once initial access is achieved.

SonicWall SMA 100 Series OS

- **CVSS:** 7.3
- **Disclosure-to-Exploitation:** Months to years (exploitation observed well after initial disclosure in multiple cases)
- **Context:** In-the-wild exploitation of SonicWall SMA 100 Series appliances used for initial access. recurring exploitation across multiple blocked ransomware campaigns, particularly in mid-market environments where appliances were internet-facing and patching lagged disclosure timelines.

  In observed activity, successful exploitation frequently yielded immediate access to valid credentials and session context, allowing attackers to bypass endpoint defenses and progress directly into lateral movement and administrative control. These intrusions often advanced from initial access to attempted encryption within a single after-hours window.

Native Tool and Administrator Abuse

Ransomware operators in 2025 continued to favor abuse of legitimate administrative and post-exploitation tooling already present in enterprise environments. Prevention telemetry and incident response observations from the year indicate that a majority of blocked ransomware activity leveraged trusted utilities rather than bespoke malware. By operating through native operating system tools, RMM platforms, and standard management interfaces, attackers reduce visibility, accelerate lateral movement, and execute coordinated, multi-host ransomware activity at scale while blending malicious actions into normal administrative behavior:

RDP (Remote Desktop Protocol)

- **Legitimate Uses:** Remote administration of Windows systems and servers
- **Abusive Applications:** Interactive access for hands-on-keyboard for lateral movement, privilege escalation, and ransomware execution across hosts
- **MITRE:** [T1021-001]

VPN (Virtual Private Network)

- **Legitimate Uses:** Remote network access for employees, contractors, and administrators using VPN gateways to authenticate and access internal resources
- **Abusive Applications:** Automated login attempts using stolen or reused passwords, especially against VPN services without multifactor authentication, to gain and maintain access
- **MITRE:** [T1110]

AnyDesk/ScreenConnect

- **Legitimate Uses:** Remote support and IT helpdesk access for endpoints and servers
- **Abusive Applications:** Covert remote control to maintain persistence, disable defenses, stage payloads, and run encryption at scale
- **MITRE:** [T1219]

Ransomware operators consistently favored native operating system utilities and trusted administrative tools over custom malware because they reduce detection and blend malicious activity into legitimate network traffic.

PowerShell

- **Legitimate Uses:** Windows automation, configuration management, and administrative scripting
- **Abusive Applications:** Discovery, downloading tools, disabling security controls, and launching ransomware without dropping obvious malicious tools
- **MITRE:** [T1059-001]

Mimikatz

- **Legitimate Uses:** Credential auditing and security testing of Windows authentication mechanisms
- **Abusive Applications:** Credential dumping to obtain passwords and hashes, enabling privilege escalation and lateral movement prior to ransomware deployment
- **MITRE:** [S0002]

WMI (Windows Management Instrumentation)

- **Legitimate Uses:** Remote system management, monitoring, and administrative automation across Windows endpoints and servers
- **Abusive Applications:** Remote command execution and lateral movement without deploying additional malicious tools, enabling attackers to execute payloads, enumerate systems, and propagate ransomware while blending into normal administrative activity
- **MITRE:** [T1047]

PsExec / RemCom

- **Legitimate Uses:** Remote administration and software deployment, including executing commands on remote systems for IT operations
- **Abusive Applications:** Remote execution for lateral movement at scale after initial access, enabling attackers to rapidly spread tooling, stage payloads, and trigger ransomware execution across multiple endpoints
- **MITRE:** [S0029]

The most reliable ransomware intrusion chain required no bespoke malware because RDP, PowerShell, WMI, and PsExec provided everything needed to move laterally, escalate privileges, and deploy ransomware at scale across an entire environment.

ProcDump

- **Legitimate Uses:** System diagnostics and troubleshooting, including capturing application memory snapshots to support debugging and incident analysis
- **Abusive Applications:** Steal login credentials from memory, enabling privilege escalation and expanded access prior to ransomware deployment
- **MITRE:** [S0422]

SharpHound (BloodHound Collector)

- **Legitimate Uses:** Active Directory security assessment and attack path analysis used by defenders and auditors to identify privilege escalation paths and misconfigurations.
- **Abusive Applications:** Rapid AD enumeration and relationship mapping to identify privileged accounts, attack paths, and lateral movement routes to domain dominance before ransomware execution. Halcyon telemetry indicates that fast, automated AD enumeration enabled attackers to precompute lateral paths and prioritize high-value systems, reducing trial-and-error movement and accelerating progression to coordinated, environment-wide ransomware execution within a single operational window.
- **MITRE:** [S0521]

Rclone

- **Legitimate Uses:** Cloud storage synchronization and backup operations across major providers, often used for legitimate data migration and redundancy workflows
- **Abusive Applications:** Data theft using supported cloud backends to move large volumes of sensitive data off-network, enabling double extortion and increasing leverage ahead of encryption
- **MITRE:** [S1040]

Eraser

- **Legitimate Uses:** Secure deletion of files and data sanitation for compliance, privacy, and device lifecycle management
- **Abusive Applications:** Evidence destruction and anti-forensics, including secure wiping of logs, tools, and artifacts to hinder investigation and complicate recovery and attribution
- **MITRE:** [T1070-004]

Hybrid Tactics

Ransomware groups in 2025 combined social engineering, infrastructure abuse, and attacks targeting cloud environments with traditional methods, resulting in hybrid intrusions observed at scale across customer environments. Across observed incidents, attackers routinely chained social engineering, perimeter exploitation, and abuse of trusted administrative tooling to compress timelines and reduce detection.

Social Engineering and MFA Abuse: Ransomware gangs impersonated help desks, used text message lures, and conducted live phone calls to trick employes into resetting passwords and multi-factor authentication for high-value accounts, including in campaigns attributed to Scattered Spider and related crews. These efforts were increasingly paired with repeated authentication prompts designed to pressure users into approving access (also known as push-based MFA fatigue) as well as phishing tools that intercepted login credentials in real time, including activity linked to Akira and other groups. [T1566] [T1078] [T1110] [T1621]

TRANSLATING INSIGHT INTO DEFENSE

Defensive Priorities

HIGHEST LEVERAGE

Identity Governance

Misconfigured service accounts and weak hybrid identity controls were the central enabler in the most damaging 2025 intrusions

BASELINE REQUIREMENT

Automated Response

69% of attacks outside business hours; human review alone will consistently arrive too late

RETHINK ASSUMPTIONS

Backup Architecture

Backups are a disaster recovery tool not a ransomware defense; attackers delete or encrypt them as a standard pre-encryption step

DECISIVE CAPABILITY

Resilience Over Prevention

Ransomware was stopped only after other controls failed; containment and recovery speed now determines who survives

69%
of attacks execute outside business hours

31%
of victims attacked more than once

22 Days
average recovery time from ransomware

Firewall and Edge-Device Lockouts: Ransomware operators in 2025 exploited vulnerabilities in internet-facing VPNs, firewalls, and secure access appliances to gain direct network access without initial endpoint malware. These devices provide authenticated connectivity into internal environments, making them high-leverage entry points when compromised. Halcyon observed ransomware attempts, including activity linked to Akira and Play, originating from compromised edge infrastructure where unauthorized VPN access was established first. In multiple cases, attackers harvested credentials, moved laterally within hours, and launched coordinated encryption during the same after-hours window, reinforcing edge-device exploitation as a fast, low-noise access path that bypasses endpoint defenses. [T1190]

Hybrid-Cloud Identity and Control-Plane Abuse: Halcyon also saw some ransomware operations move from on-premises identity systems like Active Directory into cloud environments, using compromised synchronization accounts and misconfigured application permissions to exfiltrate data, delete cloud backups, and deploy ransomware without installing traditional malware on endpoints. These operations often rely heavily on legitimate cloud management tools and automated workflows to carry out their activity, (also referred to as living-off-the-land). In mid-2025, China-linked operators and follow-on ransomware activity associated with Warlock bypassed endpoint detection entirely and attempted to execute ransomware after manipulating identity and administrative control paths rather than deploying traditional payloads. [T1078] [T1098] [T1537] [T1567]

Rapid Weaponization of Newly Disclosed Vulnerabilities: Compression of the window between public disclosure, proof-of-concept code, and use in pre-ransomware intrusion chains, including Play and Akira activity against SonicWall SSL VPN devices where fully patched appliances were compromised in suspected zero-day campaigns before fixes were widely understood or deployed. Halcyon blocked multiple ransomware executions associated with Play and Akira tied to newly disclosed edge-device vulnerabilities within days of public reporting, indicating exploitation occurring before defensive guidance was broadly operationalized. [T1190]

Repeat Victimization: Organizations that suffered one ransomware incident in 2025 continued to be more at risk for additional ransomware attacks. One report from August 2025 indicates that 31% of ransomware victims were attacked twice or more in the preceding year. Halcyon data also shows ransomware attempts recurring against previously targeted environments, including follow-on activity attributed to Akira and Play. These repeat attacks often reused the same access paths and tooling, indicating that initial access mechanisms were not fully remediated after earlier incidents.

Halcyon data shows ransomware attempts recurring against previously targeted environments, including follow-on activity attributed to Akira and Play, often reusing the same access paths and tooling, indicating that initial access mechanisms were not fully remediated after earlier incidents.

The boundaries between phishing, identity abuse, cloud exploitation, and ransomware deployment have collapsed into a single fluid attack chain that renders point solutions and siloed defenses functionally obsolete.

Outlook for 2026

As we move further into 2026, the most common attack paths are likely to stem from gaps in identity governance, exposed internet-facing systems, weak oversight of remote access and management tools, and critical environments that lack layered, defense-in-depth protections. Ransomware gangs' incorporation of AI and continued targeting of upstream providers and attempts to evade further disruptions increase the potential for more, and more sudden, attempted attacks. Organizations that prioritize containment and recovery will more successfully navigate these attempts rather than organizations that prioritize prevention alone.

Hybrid Identify and Software Platforms: Hybrid identity and software platforms are likely to become the center of gravity for intrusions. Operators will target synchronization pathways, application identities, automation credentials, and cloud backup integrations to establish durable control and limit recovery options. In the next six months, organizations are likely to see increased abuse of misconfigured applications and over-privileged service accounts, particularly where on-premises access can be extended into cloud environments. Leading indicators include unexpected changes to identity federation settings, unexpected application consent grants or credential activity, and backup configuration changes that occur before extortion attempts.

AI-Accelerated Intrusions: Over the next six to 12 months, AI is likely to increase the speed and scale of ransomware operations more than it changes core tradecraft. Ransomware actors will continue to use generative AI to streamline discrete tasks including phishing, translation, vulnerability analysis, and tool modification. Agentic AI will remain limited to narrow workflows and early-stage experimentation. Defenders should expect shorter patch-to-exploit windows, more tailored social engineering, and faster iteration when attacks encounter controls. Most organizations will also likely experience an increase in ransomware attempts from low-sophistication actors, increasing the potential for security team fatigue and burnout.

Upstream Providers: Ransomware gangs will continue targeting upstream providers, including managed service providers, IT and security tooling, and widely used enterprise platforms to gain scalable access. A single breach at this level can open access to dozens or even hundreds of downstream organizations at once. Over the next six months, organizations should expect sudden clusters of victims tied to the exploitation of a small number of internet-facing platforms. Initial access will often originate outside the victim's perimeter, reducing early detection opportunities. Warning signs include unusual administrative activity through vendor tools, unexpected remote management agents appearing across multiple environments in rapid succession, and similar initial access intrusion patterns surfacing across otherwise unrelated organizations.

Over the next six to 12 months, AI is likely to increase the speed and scale of ransomware operations more than it changes core tradecraft

Stronger OPSEC and Less Visible Leak Infrastructure: As enforcement pressure targets high-visibility brands, operators are hardening operations by rotating infrastructure faster, relying more on brokered channels, and reducing dependence on public leak sites. This trend complicates ecosystem visibility, particularly where counting methodologies rely heavily on leak-site monitoring rather than direct telemetry. Over the next six to twelve months, expect a larger share of extortion flows that never touch a public leak site, increased use of private negotiation channels, and more unstable or short-lived leak infrastructure. Leading indicators include extortion demands delivered without prior public signaling, direct transmission of proof packages to victims, and declining consistency between public leak postings and observed intrusion activity.

Defensive Gaps Most Likely to Be Exploited: Taken together, Halcyon analysis and authoritative public reporting indicate that the most reliable attack paths in 2026 will remain misconfigured identity and SaaS control planes, exposed perimeter infrastructure, weakly governed remote access, and RMM tooling, and under-segmented backup and recovery stacks. Organizations should monitor consolidation and fragmentation signals, track after-hours access and execution patterns, and prioritize controls that reduce attacker speed and reliability, particularly across identity, remote administration, and recovery architectures.

Methodology

This analysis reflects a blended assessment of ransomware activity observed during calendar year 2025, integrating large-scale prevention telemetry, incident response observations, and threat intelligence analysis with qualitative evaluation of attacker tradecraft, operational behavior, and ecosystem dynamics. The findings are informed by the combined work of Halcyon threat intelligence, research, reverse engineering, and product engineering teams, as well as insights shared through collaboration with industry partners and security teams operating within customer environments.

The methodology combines quantitative observation of ransomware activity across protected environments with qualitative analysis of intrusion behavior across the attack lifecycle. Quantitative inputs include encryption attempts stopped on endpoints, detection of earlier-stage behaviors occurring prior to encryption, and telemetry associated with access, identity abuse, tooling usage, lateral movement, and data exfiltration. These observations are analyzed in aggregate to identify recurring execution patterns, timing characteristics, and operational dependencies rather than isolated incidents.

Qualitative inputs are derived from hands-on incident analysis, reverse engineering of tooling and payloads, and structured review of intrusion workflows observed across multiple environments. These assessments are supplemented by publicly available information compiled from authoritative open sources, including government advisories, industry reporting, and verified disclosures, which are used to contextualize and validate observed trends rather than serve as the primary basis for conclusions. Reasonable efforts were made to sanitize, validate, and cross-check all underlying data; however, no guarantee is made regarding accuracy, completeness, or reliability, and the analysis reflects conditions observed at the time of publication.

This report is provided in accordance with principles of fair use and is updated as new information becomes available from reputable sources. By accessing or using this report, readers acknowledge that it is intended for informational and analytical purposes only and should not be relied upon as the sole basis for decision-making. Halcyon disclaims liability for any inaccuracies or omissions arising from the use of this material.

Other Sources Consulted

https://www.halcyon.ai/attacks

https://www.thecannatareport.com/ransomware-attacks-soar-by-45-percent/

https://www.ransomware.live/

halcyon

Detect. Disrupt. Defeat Ransomware.™

Ransomware isn't just another threat. It's a different category of attack. Experienced security leaders need tools that match their readiness. 'Mostly sufficient' security is no longer sufficient when facing AI-powered ransomware. With 91% already exploring ransomware specific tools following high stakes incidents and boards demanding answers, the shift from general-purpose security to purpose-built ransomware defense is no longer optional; it's imperative.

The Halcyon Ransomware Research Center unites experts, drives smart policies, and delivers actionable intelligence to detect, disrupt, and defeat ransomware.

Explore the Center's latest reports, analysis, and resources here.