Securin

Ransomware Index Report 2025

Ransomware isn’t just evolving, it’s mutating.

Introduction

WHEN RANSOMWARE BECAME HYBRID WARFARE

What we learned in 2025: Ransomware isn’t just evolving, it’s mutating.

Last year, we warned that ransomware was no longer *just* about encryption. It had evolved into a contest of control, persistence and psychological pressure – a trend amplified by the arrival of GenAI-enabled tooling and techniques.

In 2025, that warning feels almost understated. This year, ransomware crossed a threshold, targeting the layers of infrastructure that hold entire organizations together: ESXi hosts, hypervisors, Fortinet perimeters, SharePoint ecosystems and Unified Extensible Firmware Interface (UEFI) trust chains. Attackers are moving beyond single vulnerabilities to precise exploitation chains designed for maximum impact.

This was the year criminal operators adopted Advanced Persistent Threat (APT) group-grade discipline, chained multi-layer vulnerabilities across entire platforms and shifted focus from endpoints in favor of the infrastructure that keeps organizations working.

Securin’s analysis of 7,061 confirmed victims, across 117 groups, reveals a threat ecosystem expanding in size, but consolidating in power. Groups such as Akira (650 victims), Qilin (835 victims) and CL0P (517 victims) act as apex predators.

Their rise mirrors a pattern we first saw emerging in 2024: ransomware groups acting less like opportunistic gangs, and more like decentralized, resilient enterprises.

What's keeping us up at night

1 **AI is industrializing ransomware**
GenAI isn't running campaigns autonomously, but it is compressing the economics of ransomware. By reducing friction across development, access and extortion, AI is turning ransomware into a higher velocity, higher volume business.

2 **Hybrid threat actors have taken over**
The Big Three - Qilin, Akira and CL0P - now operate with APT-like structure and persistence - decentralized affiliates, mature playbooks and strategic targeting.

3 **Trust has become the primary attack surface**
Ransomware campaigns shifted to hypervisors, collaboration platforms and identity systems. Compromise no longer *just* disables devices; it disables entire organizations.

4 **Commercial facilities are the new #1 target**
With this sector accounting for 14% of confirmed victims, it's clear that attackers are now hunting where impact is public, leverage is immediate, and operational downtime is expensive.

5 **Exploitation chains are rewriting the playbook**
Multi-Common Vulnerabilities and Exposures (CVE) exploits across SharePoint, Fortinet, ESXi, UEFI and legacy drivers reveal a tactical shift: attackers aren't just exploiting vulnerabilities, they're orchestrating them.

6 **Ransomware and information warfare converged**
The Department of Government Efficiency (DOGE) Big Balls campaign fused extortion with conspiracy narratives via targeted doxxing and psychological pressure, turning technical attacks into influence operations.

BOTTOM LINE

Ransomware in 2025 behaves less like cybercrime and more like a coordinated campaign to undermine digital trust. Attackers no longer settle for access; they seek leverage, selecting the weaknesses that present maximum reach, maximum disruption, and maximum psychological pressure.

By targeting virtualization layers, identity systems, collaboration platforms and the trust systems underpinning today's enterprises, adversaries have created a shift that required organizations to rethink defensive models entirely, from perimeter prevention to trust-centric, infrastructure-aware resilience.

What's in this report

"In 2025, AI turbocharged ransomware economics by accelerating vulnerability weaponization—from rapid discovery and exploit crafting to intelligent multi-vector chaining (AI-powered phishing for entry, identity compromise for escalation, exploits for propagation)—maximizing compromise scale and extortion ROI at machine speed.

Defenders must counter with AI-driven proactive resilience: prioritized vulnerability management, strong identity controls, deception, and autonomous hunting to break these efficient attack chains before they cascade.

The advantage belongs to those who deploy defensive AI faster than adversaries weaponize offensive AI."

SRINIVAS MUKKAMALA, PHD.
SECURIN CHIEF EXECUTIVE OFFICER

AI x Ransomware

Deconstructing the AI convergence

One of the most visible developments in 2025 was the growing use of generative AI in ransomware operations. It's also one of the most overstated.

AI hasn't replaced human operators, or become an autonomous driver of ransomware campaigns - but it has emerged as a force multiplier. It accelerates workflows, lowers barriers to entry, increases scale and heightens the psychological impact.

TL;DR

The core logic of modern ransomware remains human-directed. What's changed is speed, reach and efficiency.

Where information warfare like DOGE Big Balls expanded ransomware's psychological reach, AI is expanding its operational speed, automation and attack surface. Across the campaigns Securin observed, AI contributed meaningfully in four operational domains:

- **Code generation**
- **Adaptive execution**
- **Social engineering**
- **Negotiation automation**

Hype meets reality: separating the signal from the noise

Early 2025 reports that most ransomware attacks were “AI-driven” drew heavy criticism from the security research community. The main culprit driving this wasn’t hype, so much as conflating access to AI tools with operational dependence on AI. Threat intelligence consensus is much more grounded: AI is supportive rather than orchestrational.

Threat actors routinely use AI to draft phishing messages, debug scripts and translate content, but only a small number of cases in 2025 crossed the threshold into AI-dependent execution.

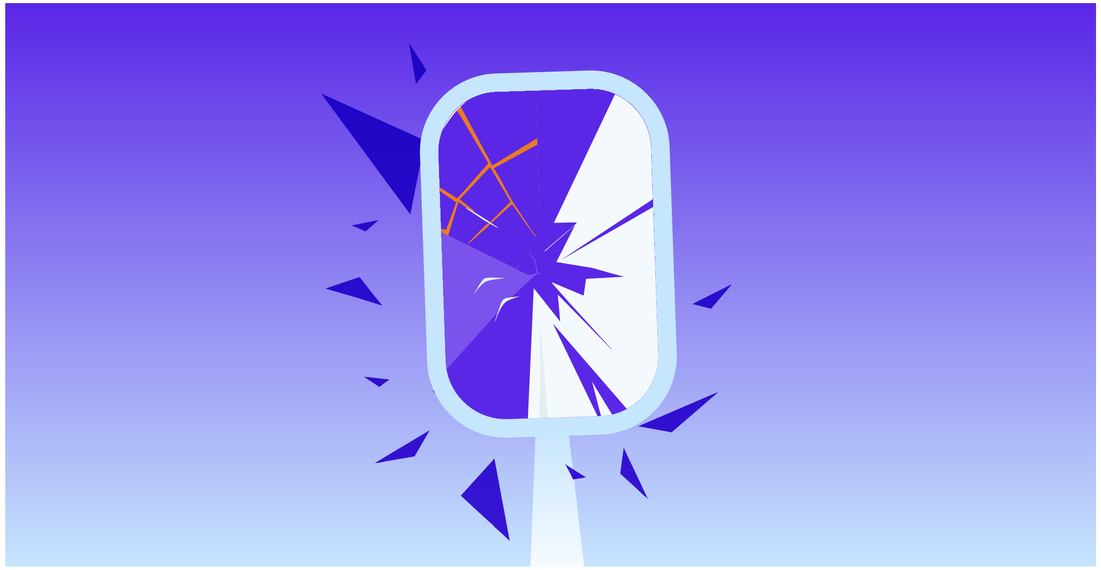
BOTTOM LINE

The real story isn’t autonomous ransomware, it’s accelerated ransomware - driven in no small part by low barrier to entry.

What does that look like?

Deepfakes and the trust gap: Identity as attack surface

2025 marked a turning point in identity-based social engineering: the collapse of “seeing is believing” in initial access. Deepfake audio and video moved from novelty to operational tradecraft, narrowing the gap between fraud, access and ransomware deployment.



Code generation: The FunkSec pattern

As Securin identified in last year’s report, FunkSec offers the clearest example of AI lowering the barrier to ransomware. Since emerging in 2024, the group has scaled rapidly, despite limited operator skill.

Forensic analysis of its Rust payload revealed hallmarks consistent with LLM-assisted coding, including:

Highly polished English language comments that contrast with poor operator language in ransom communications.

Redundant or fragile logic, typical of unoptimized AI output.

Rapid version iteration exceeding normal manual development pace.

FunkSec demonstrates a practical shift: intermediate actors can now ship modern ransomware without needing deep engineering expertise. AI doesn’t make these groups elite - it makes them viable. This increases attacker volume, experimentation and baseline capability across the ecosystem

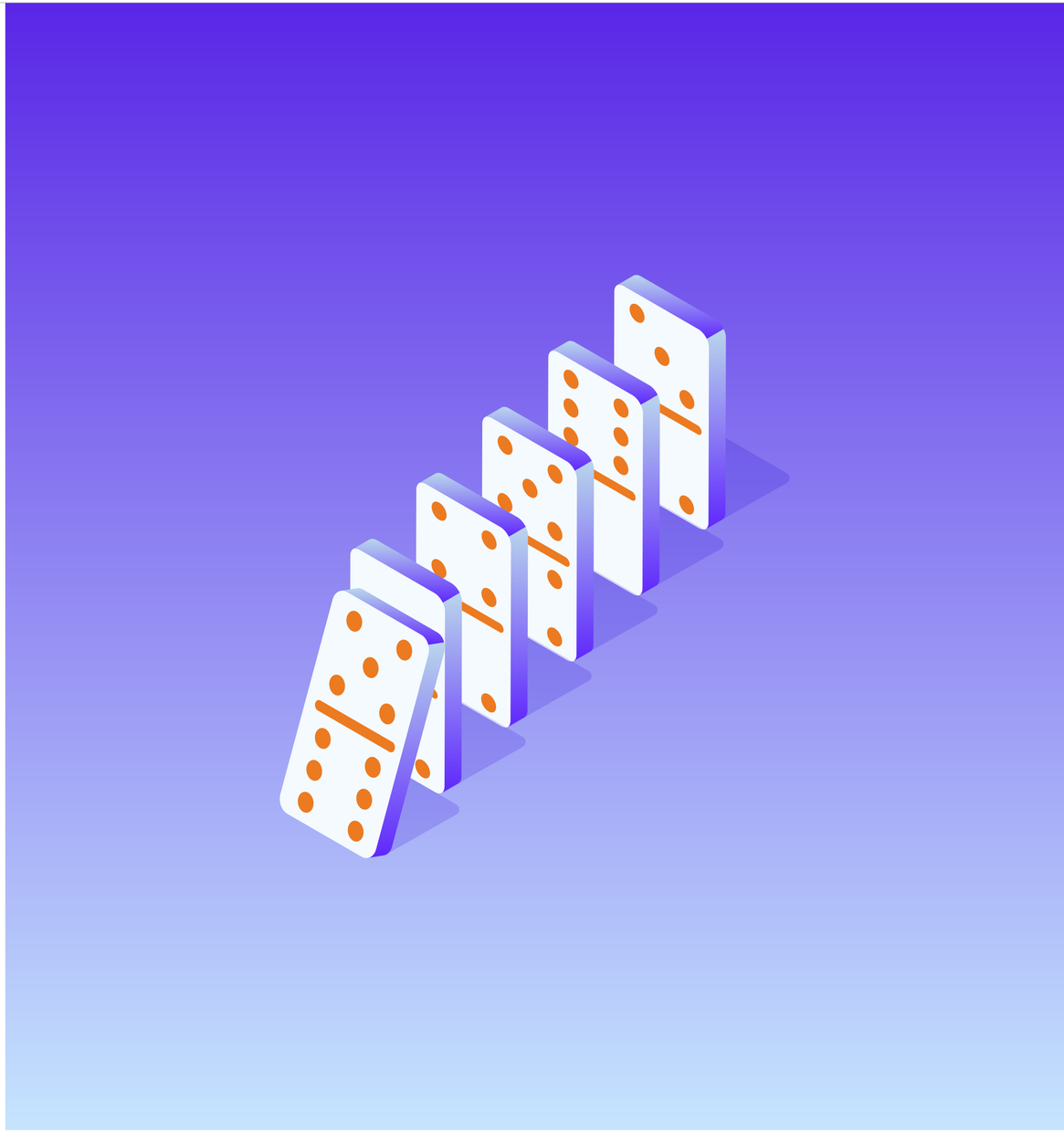
Dynamic execution: PromptLock and LameHug

A more consequential evolution appeared in mid-2025: malware using AI at runtime, not just during development. While still early-stage, PromptLock validated the feasibility of adaptive ransomware that changes behavior according to the victim environment.

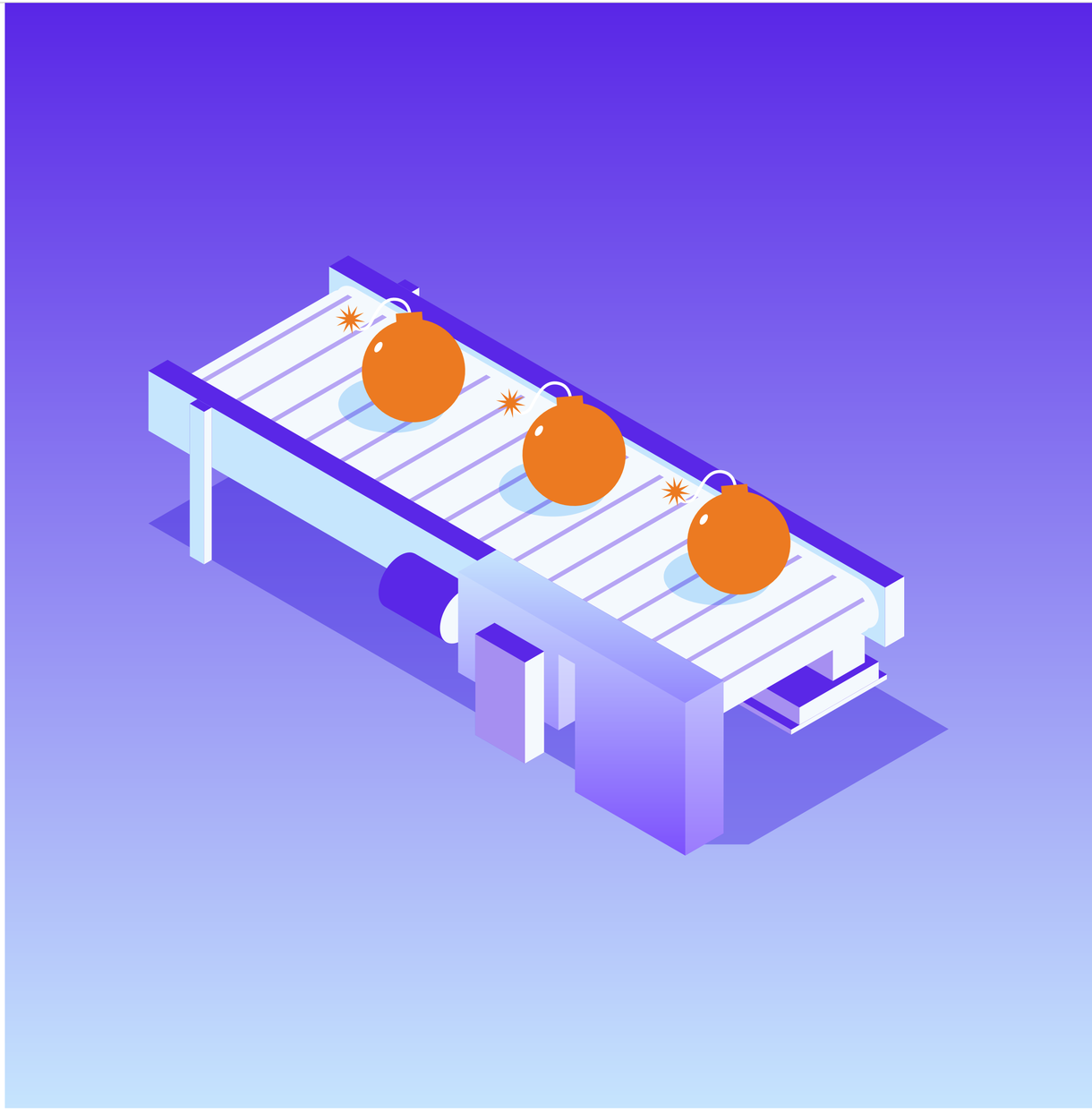
It embeds a locally hosted LLM, generating malicious scripts dynamically during execution. Instead of shipping fixed logic, PromptLock issues natural-language prompts that produce runtime-specific attack code. This creates polymorphic execution paths that weaken signature-based detection.

A parallel pattern appears in LameHug, an AI-assisted infostealer linked to threat group APT28. It uses an LLM to translate vague operator intent into precise, environment-specific commands, allowing living-off-the-land activity without continuous human control.

Together, PromptLock and LameHug show where AI becomes strategically meaningful: not by developing malware faster, but by making it more adaptive.



Automating extortion: Global Group’s negotiation bots



2025 also saw AI re-shaping the business of ransomware: threat actor Global Group automated victim communications using AI chatbots inside Tor-based negotiation portals. These bots handle onboarding, payment instructions, file verification and scripted psychological pressure.

The operational impact: scale. Groups can now manage hundreds of concurrent extortion cases, with minimal ‘staffing’. Language barriers have also collapsed thanks to automated translation, enabling broader affiliate expansion and more convincing global victim engagement.

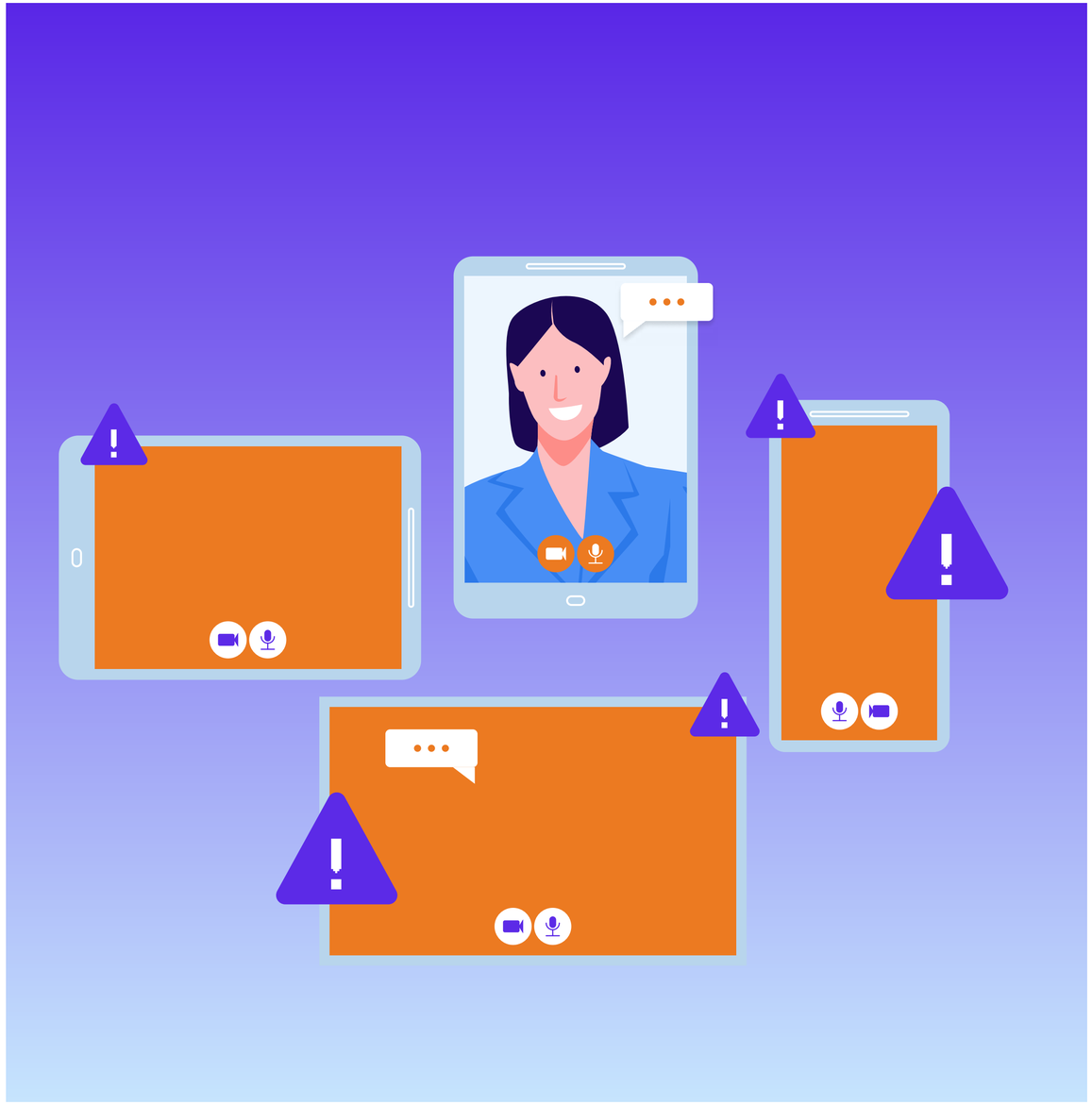
BOTTOM LINE

Ransomware isn’t just becoming more technical, it’s becoming more operationally industrialized.

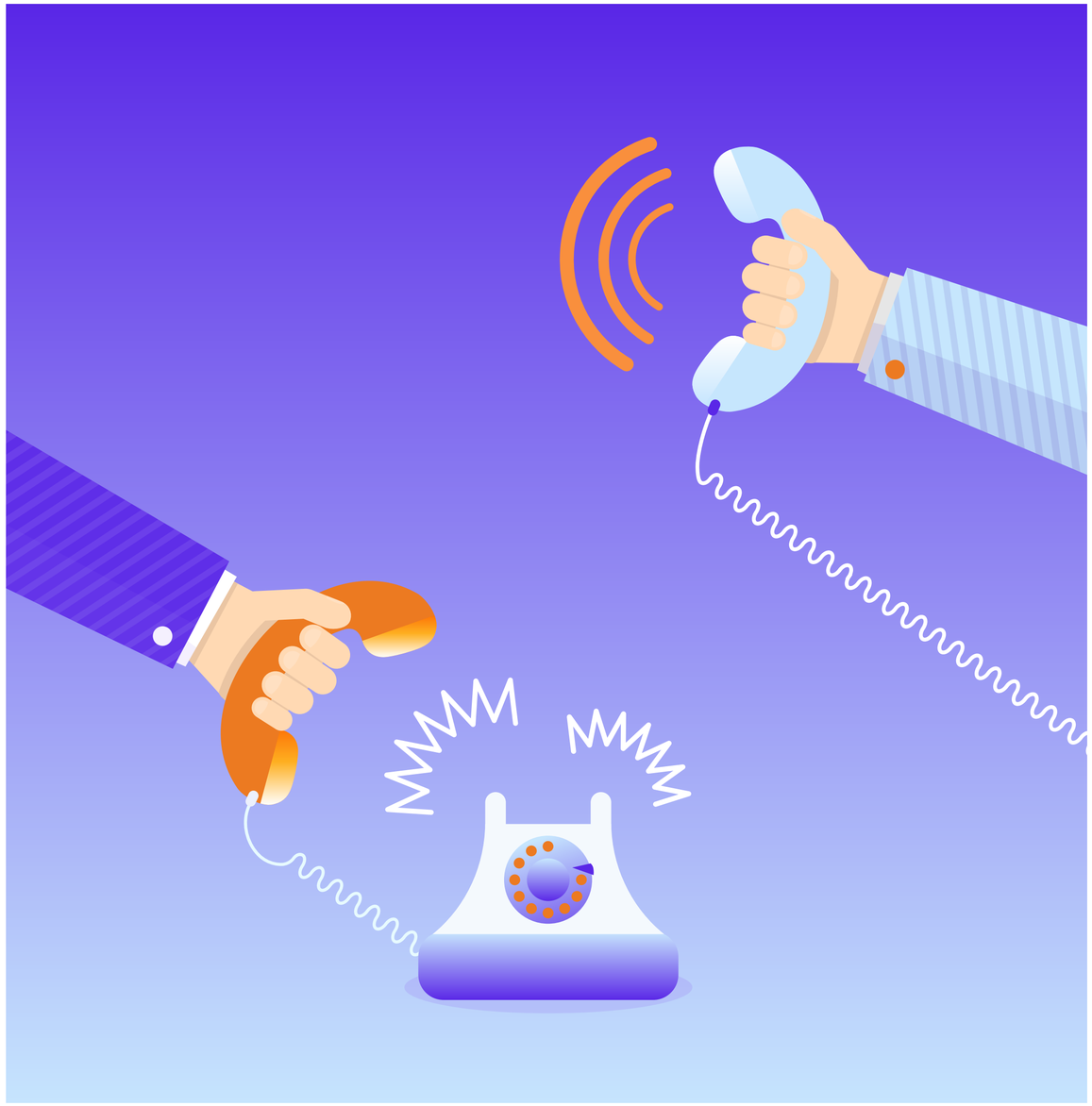
Arup: a $25m warning

The Arup breach illustrated the new trust failure model when a finance employee approved a major transfer after joining a video call featuring what appeared to be company executives. All ‘participants’ except the victim were AI-generated deepfakes.

This incident demonstrates a structural shift: video verification can no longer be treated as proof of authenticity. Identity itself has become spoofable in real time.



Scattered Spider and AI-driven vishing



Groups such as Scattered Spider have integrated voice cloning into routine access operations, using short audio samples harvested from voicemail or public content to impersonate executives or helpdesk staff.

What this means: attackers now used cloned voices to request MFA (multifactor authentication) resets or credential changes, then pivot into ransomware deployment.

Once again, the key shift is scale: AI collapses the dependency on highly skilled social engineers, making identity deception relatively simple, repeatable, fast - and high-volume.

BOTTOM LINE

The ransomware attack surface has expanded from systems to human trust infrastructure.

What this means in 2026

What we learned from 2025: AI is not the strategy, it's the accelerator.

Across code development, adaptive execution, social engineering and automated extortion, AI is amplifying the same forces already reshaping ransomware: infrastructure targeting, trust exploitation, psychological pressure, and economic optimization.

The most successful ransomware groups in 2025 were not defined by their tools, but by their structure, discipline and strategic intent.

Those dynamics come into sharp focus when we examine the operators who now dominate the ransomware ecosystem.

AI didn't replace ransomware operators. It made them faster, cheaper and more scalable.

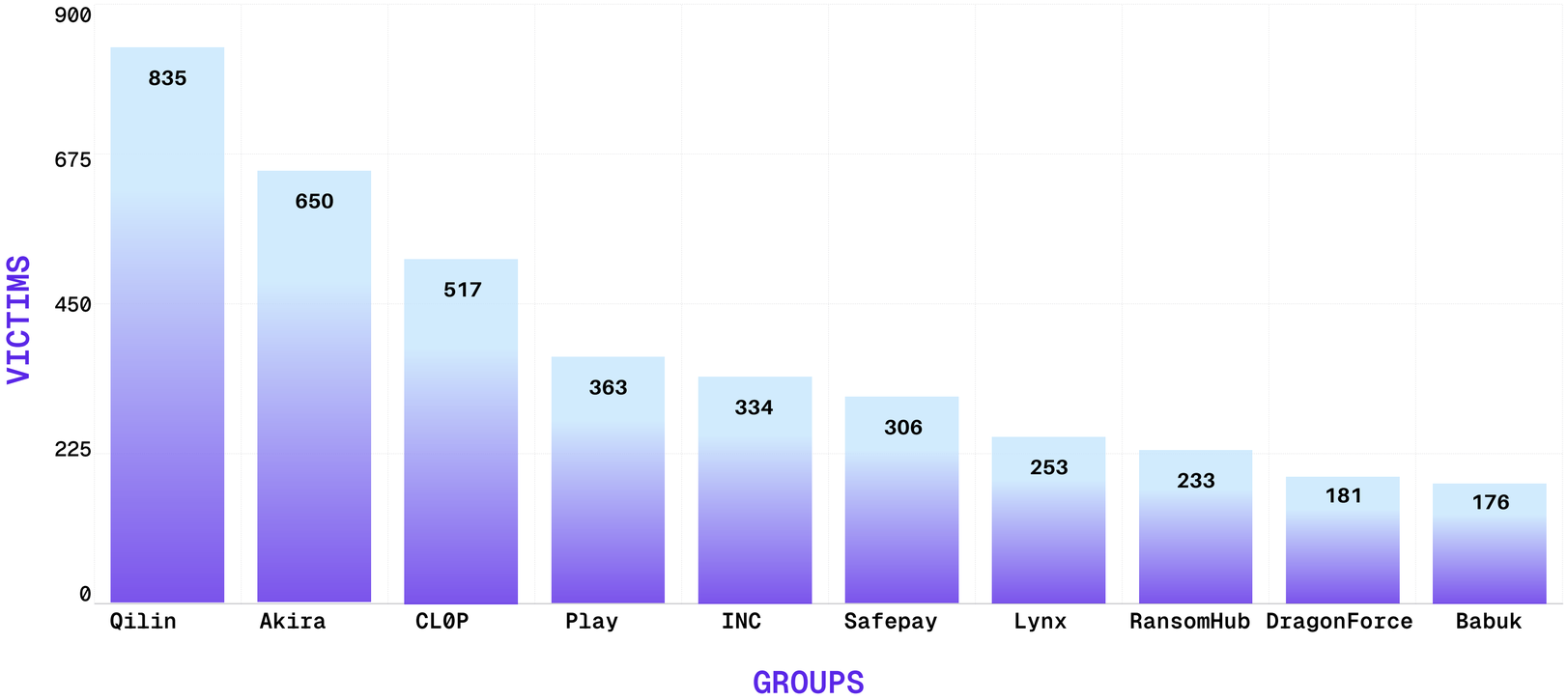
The real impact of AI is acceleration, not autonomy.
Attackers use it to generate code, craft lures, automate negotiations and adapt on the fly.

Barriers to entry collapsed in 2025.
Groups like FunkSec proved that mid-tier actors can now ship modern ransomware with minimal expertise.

The attack surface moved from systems to identity.
Deepfakes and AI-driven vishing turned human trust into a new point of failure.

The rise of hybrid threat actors

Hybrid Threat Actors: Where crime meets statecraft



With ransomware groups, the only real certainty is change. But in 2025, we saw something fundamentally different: the emergence of operators that no longer behave like criminal gangs, but like distributed, intelligence-driven organizations. Their structure, discipline and operational resilience reveal a shift from financially motivated disruption to one of strategic coercion.

With organizational structures that wouldn't look out of place in a state-sponsored threat-matrix, 2025's groups blend the agility of de-centralized insurgent cells with the operational discipline and flex of venture-backed startups: core developers, affiliate "sales" organizations, specialist exploit suppliers and negotiators who treat extortion as structured dealmaking – all with intelligence functions that map targets long before intrusion begins.

This is no longer about opportunistic cybercrime, it's hybrid threat activity, defined by capability, intent and the ability to weaponize infrastructure-level leverage.

Three groups define this transformation:

Qilin **Akira** **CL0P**

Qilin: The Linux whisperer

Qilin's rise - 835 confirmed victims - isn't simply the story of a prolific actor. It's the clearest example of a ransomware group embracing an infrastructure-first strategy.

Qilin has built an empire on Linux and ESXi mastery, proving that, in 2025, the most valuable real estate wasn't the endpoint, but the virtualization layer. The group's playbook is optimized for environments where downtime = systemic paralysis. Qilin understands what many defenders still underestimate: if you own the hypervisor, you own the business.

An encrypted ESXi host doesn't take a single system offline, it freezes dozens of virtual machines simultaneously:

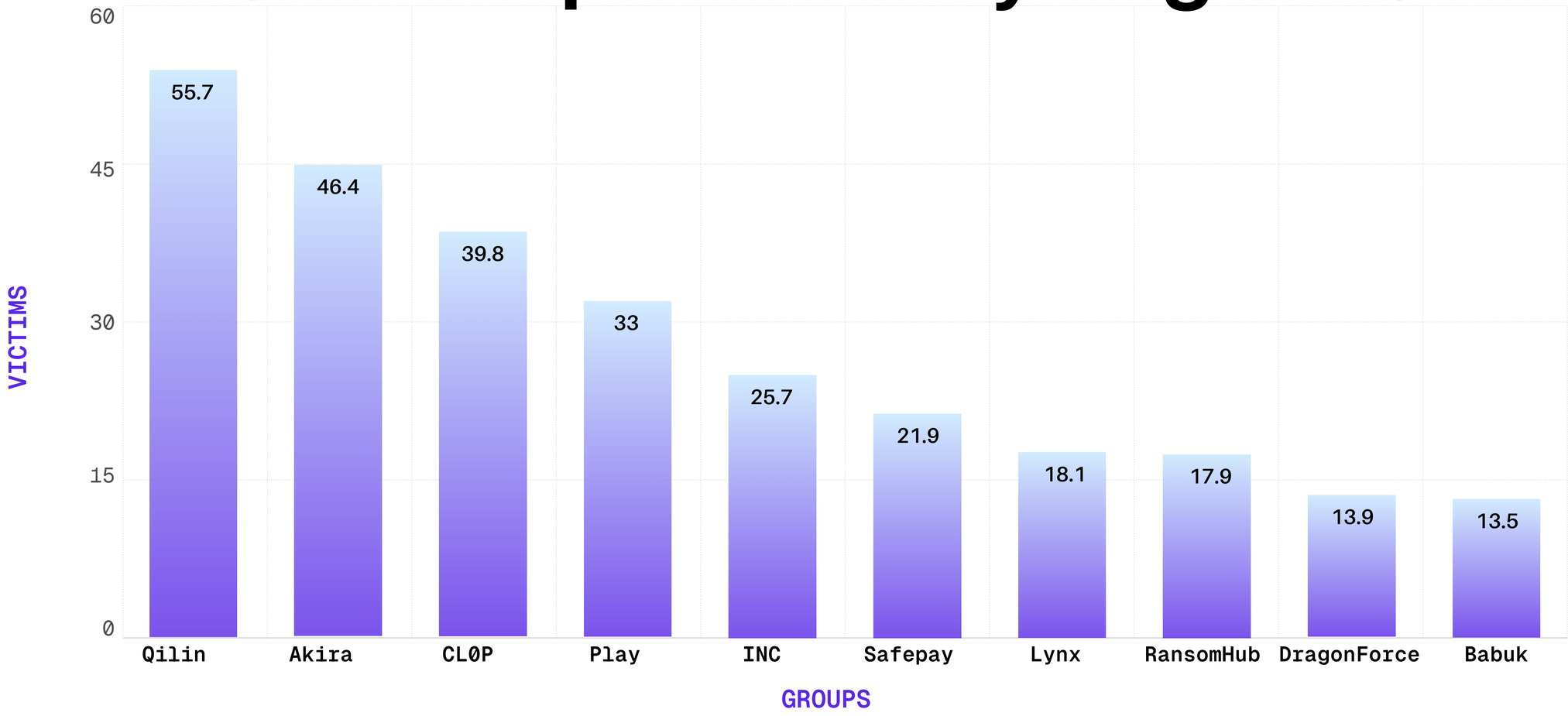
- **Enterprise Resource Planning (ERP) systems**
- **Clinical systems**
- **Industrial controllers**
- **Data platforms**
- **Core business applications**

This focus signals a maturation of attacker tradecraft. It mirrors state-level adversaries that seek choke points, not access points, and underscores a shift from opportunistic infection to infrastructure leverage.

MO

Identify the dependency that matters most, and strike there.

Group efficiency (victims per industry targeted)



Akira: The cross-sector chameleon

Each intrusion appears calibrated to the target's environment - sector, tech stack, identity architecture and business model - making Akira less like a criminal gang and more like a consulting firm executing bespoke operations. This is not high-volume spray-and-pray ransomware. This is a targeted intrusion methodology.

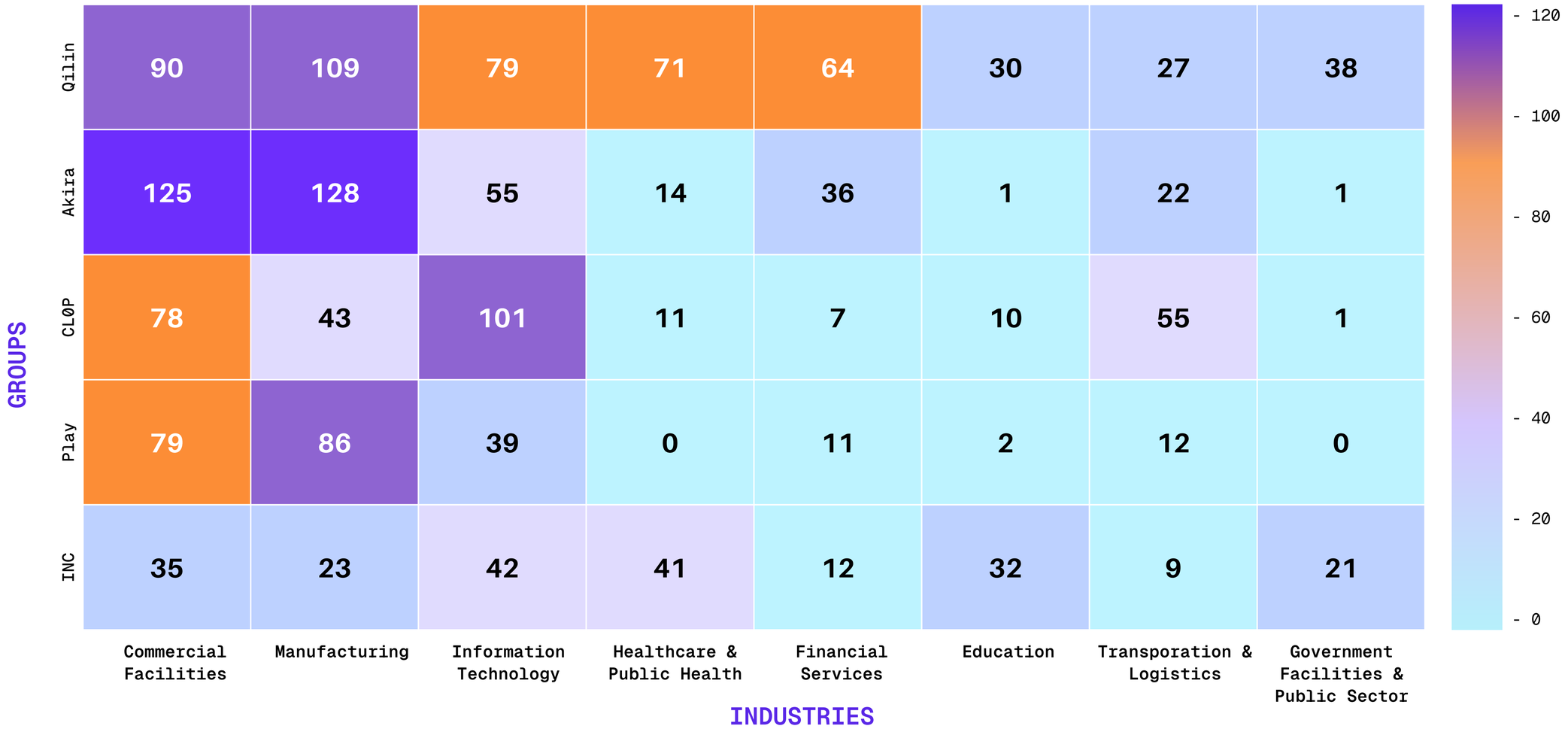
MO

This is a model we've come to associate with nation-state actors - targeted, informed and proportionate to the victim's operational dependencies.

If Qilin's strength is technical leverage, Akira's is operational intelligence and adaptability. Their footprint - 650 victims across 14 industries - suggests a repeatable, industrialized process for reconnaissance and pre-attack intelligence:

- Rapid infrastructure mapping
- Business process profiling
- Vulnerability correlation
- Tailored attack design
- High-leverage timing of encryption events

Group-industry impact matrix



CL0P: The resilient phoenix

CL0P's persistence - 517 victims in 2025, despite sustained law enforcement action - underlined how modern ransomware groups are re-organizing into cell-based operational structures.

Proving that dismantling infrastructure doesn't dismantle capability, the group's tooling, tradecraft and negotiation playbooks survive even when infrastructure and leadership are disrupted. When one cell burns, another continues or takes its place.

This de-centralization mirrors attributes we've seen in the Democratic People's Republic of Korea (DPRK) and People's Republic of China (PRC)-linked campaigns Securin analyzed this year:

- Leadership that's functionally replaceable
- Capability persisting long after disruption
- Cells sharing tooling but acting semi-autonomously
- Campaign themes that continue through successor operators

CL0P is no longer a group; it's an ecosystem that is resilient not because it hides, but because it fragments. It changes the defender's problem because shutting down servers or disrupting one node doesn't shut down the operation, the ecosystem simply reconfigures around the loss.

MO

Operates through a cell-based affiliate model - it distributes tooling, negotiation playbooks, target lists and operational guidance across semi-autonomous cells

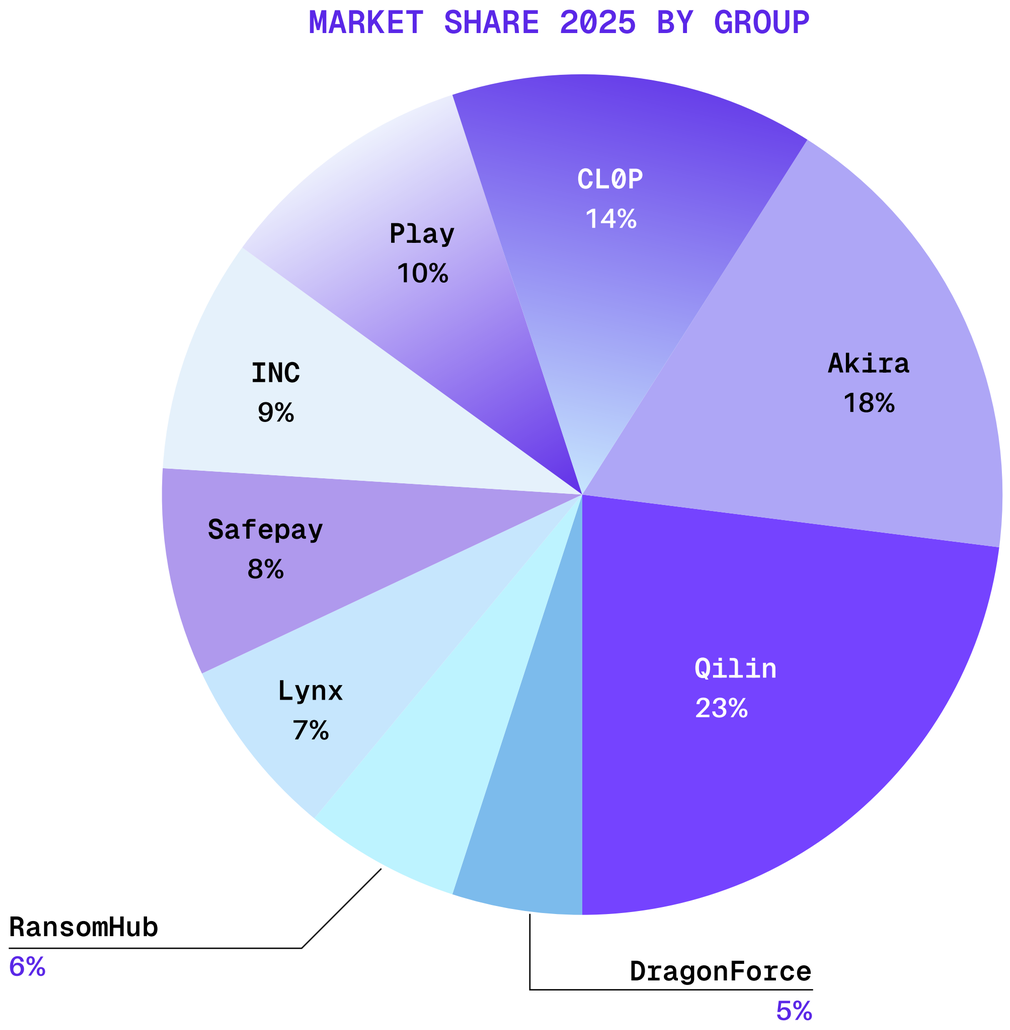
How three groups bent the ransomware ecosystem around them

Our data reveals a fascinating paradox: while the number of active ransomware groups expanded to 117, the ‘market’ itself consolidated around Qilin, Akira and CL0P.

This concentration isn’t solely due to technical sophistication, it also underlines a powerful network-effect economy of cybercrime:

Successful groups attract the most capable affiliates. Capable affiliates produce more successful compromises. More successful compromises generate higher revenues. Higher revenues enable better tooling, recruitment and innovation.

This positive feedback loop has created a cybercriminal aristocracy - a small cluster of hybrid threat actors whose scale, resilience and operational maturity are now self-reinforcing.



What it means for defenders

Qilin, Akira and CL0P aren't outliers. They're the blueprint for the next generation of ransomware power, and their rise signals the stakes defenders must now plan for.

Market consolidation exposes a deeper strategic shift: the line between a criminal group and a hybrid threat actor is no longer defined by capability, it's defined by sponsorship and intent. And both are increasingly opaque.

For defenders, this ambiguity matters. Responders can no longer assume they're facing a purely financially motivated adversary. Every intrusion must now be treated as if:

- The attacker could behave like a state-level operator
- A campaign could be part of a broader, distributed ecosystem
- Intrusions may target infrastructure rather than data
- The ransom note may just be one piece of a bigger coercive strategy.

Where the attacks hit hardest

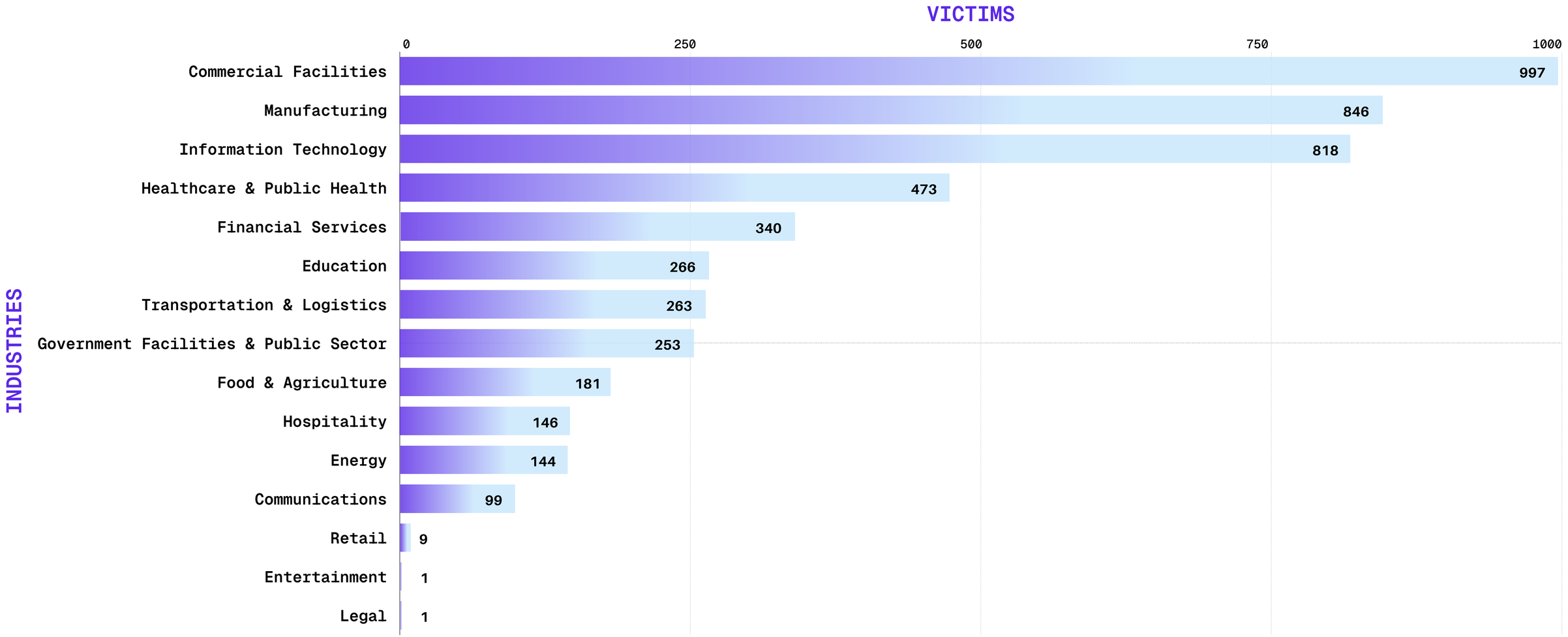
Sectoral apocalypse: Industries under siege

Across all industries, one pattern defines ransomware in 2025: Attackers didn't go where defenses were weak, they went where disruption would be impossible to ignore - the sectors where operational exposure, public visibility and systemic dependency create maximum leverage:

- Commercial facilities maximize visibility
- Manufacturing maximizes systemic consequences
- IT maximizes blast radius
- Healthcare maximizes urgency
- Government and public sector maximizes institutional disruption

These are not random choices. They're strategic selections consistent with hybrid threat logic, where the goal is not simply data encryption, but to inflict maximum pressure across operational, psychological and societal layers

Ransomware victims by industry



Sectoral targeting: 2024 vs 2025

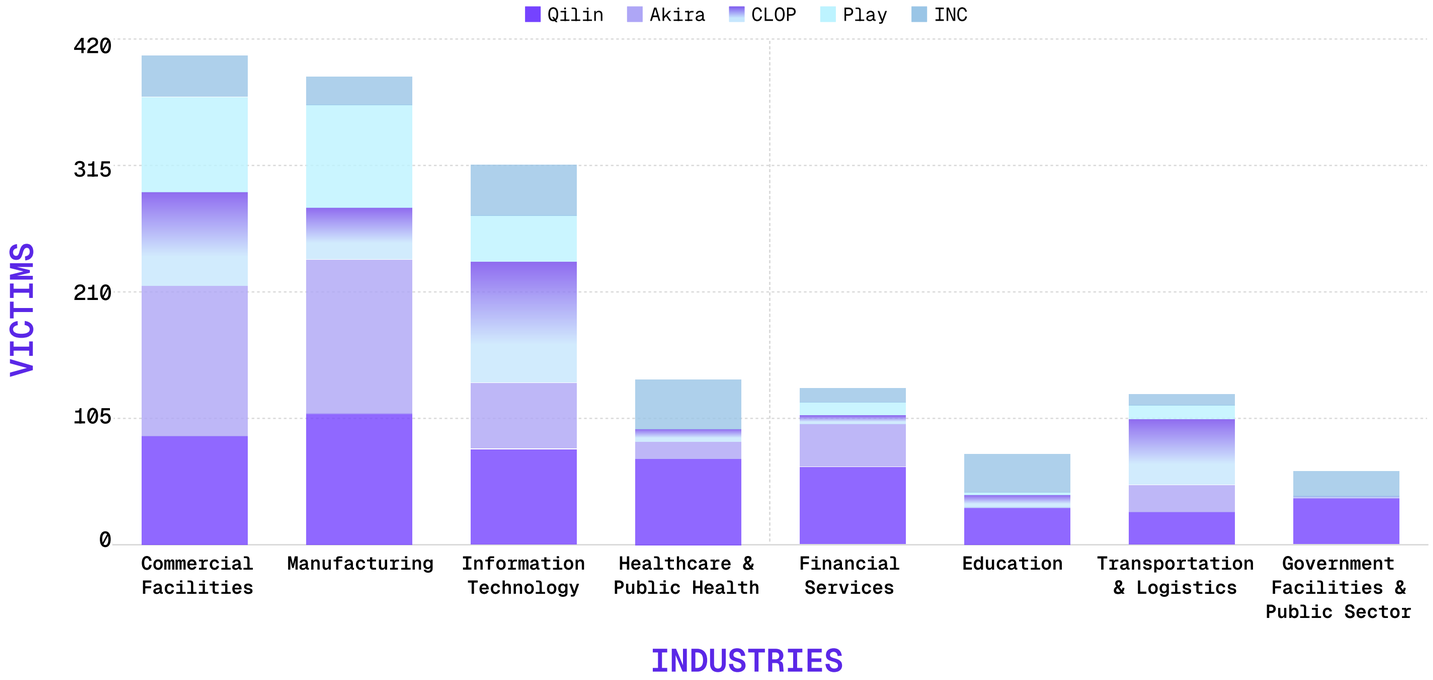
BOTTOM LINE

2025 targeting reflects hybrid threat logic - sectors are chosen for pressure yield, not technical convenience.

SECTOR	2024 PATTERN	2025 PATTERN	WHAT CHANGED & WHY IT MATTERS
Commercial Facilities	Secondary target; opportunistic attacks tied to exposed systems and retail IT.	Primary target (997 victims, 14.1%). Highly visible, high-pressure environments.	Shift from opportunism to leverage economics. Visibility and public disruption now amplify ransom pressure.
Manufacturing	Rising target (9.1% of attacks). Focus on IT-side compromise with downstream disruption.	Cyber-physical warfare (846 victims). Direct impact on production, logistics, safety systems.	Attackers move from data loss to operational paralysis and supply-chain impact.
Information Technology	Consistent targeting due to access to downstream customers.	Meta-target (818 victims). MSPs, SaaS, cloud, integrators directly exploited.	Compromise of IT providers used as blast-radius multipliers.
Healthcare & Public Health	Most targeted sector (14.5%). Ethical restraints beginning to erode.	Still heavily targeted (473 victims). Restraints largely gone.	Healthcare is now treated as high-leverage infrastructure, not a protected domain.
Government & Public Sector	Regular target, often via exposed services.	253 victims, with collaboration platforms as entry points.	Shift toward workflow and coordination disruption, not just system access.
Overall Targeting Logic	Volume-driven, sector familiarity.	Strategic, pressure-optimized targeting.	Attackers select sectors based on visibility, urgency, and systemic consequence, not ease alone.

Commercial facilities: High-visibility pressure points

TOP 5 GROUPS IMPACT ACROSS INDUSTRIES



With 997 confirmed victims (14.1%), commercial facilities were ransomware's primary hunting ground in 2025. This sector – including shopping malls, hotels, arenas, convention venues and large retail infrastructure – provides the perfect combination that hybrid threat actors are looking for:

Broad, heterogeneous attack surfaces

Point of Sale (POS) systems, building management networks, Heating, Ventilation, and Air Conditioning (HVAC) controllers, digital signage, supply chain interfaces, loyalty platforms and guest Wi-Fi form sprawling, interdependent attack planes.

Inconsistent security maturity

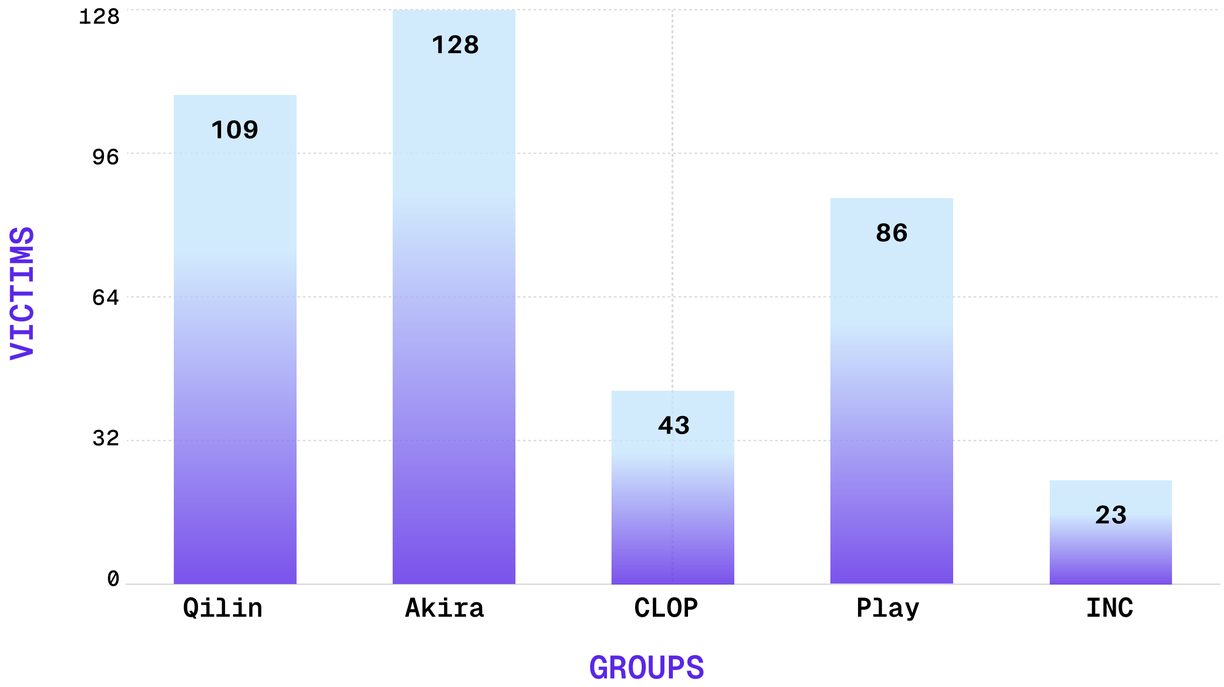
Many operators run decentralized IT teams, outsourced management and mixed-age infrastructure, increasing the likelihood of exploitable weakness.

Immediate public impact

When a hotel chain or shopping mall loses operational control, hundreds or thousands of people see it. That visibility creates leverage.

Akira's 125 victims in this sector underscores its 'high-impact, low-complexity' doctrine: strike where the outage can become its own pressure amplifier.

Manufacturing: Cyber-physical warfare



The 846 manufacturing victims in 2025 indicate a fully realized shift into cyber-physical compromise. Intrusions no longer stop at encryption, they extend into:

- Production line automation
- Robotics and PLC networks
- Supply chain orchestration
- Industrial scheduling and quality control systems
- Safety instrumentation

Manufacturing networks blend traditional IT with operational technology (OT), ICS protocols and proprietary hardware – and environment where segmentation is difficult and patching is often operationally risky.
Akira's 128 manufacturing victims suggest a deliberate operational investment in understanding ICS-adjacent tradecraft. This pattern mirrors the behavior of state-linked actors targeting energy and heavy industry – but at ransomware scale and speed.

THE SUPPLY CHAIN MULTIPLICATION EFFECT

The key takeaway here is that a ransomware event in manufacturing is no longer simply an IT issue, it's a production outage with immediate economic and safety implications that resonate throughout supplier networks. A single automotive parts manufacturer can disrupt vehicle production across multiple countries. This multiplication effect creates significant pressure for rapid incident resolution, often resulting in ransom payments that exceed the direct costs of business interruption.

Information Technology: The ironic victim

Few sectors embodied the sophistication of ransomware campaigns in 2025 like IT itself. With 818 victims, the very organizations we expect to understand cybersecurity threats most comprehensively found themselves disproportionally targeted and successfully compromised.

IT's ransomware story in 2025 highlights a painful truth: complexity is a vulnerability multiplier. IT providers, MSPs, MSSPs, SaaS vendors, cloud integrators and hosting organizations operate environments where:

- Multi-tenancy is normal
- Change rate is high
- Tooling stacks are dense and overlapping
- Customer trust is implicit

This complexity creates what security researchers term "Emergent Vulnerabilities": security gaps that emerge not from any single system weakness, but from the complex interactions between multiple secure systems.

With 101 IT sector victims in 2025, CL0P's dominance illustrates its evolution into "meta-attacker" – adversaries specializing in compromising the companies responsible for securing others. The blast radius cascades though shared environments, inherited integrations, privileged-access channels and software update pipelines. This requires both technical sophistication and deep operational understanding.

As Securin's researchers observed in our Democratic People's Republic of Korea (DPRK) and People's Republic of China (PRC) reports: Compromise the hub, and the spokes follow.

Healthcare and Government: Attacks on society's foundation

Although commercial facilities claimed the highest share of victims, the impact on healthcare and government is arguably more severe. With 473 successful attacks on healthcare & public health, and 253 government facilities, 2025 marked a qualitative shift from profit-motivated attacks to ones threatening fundamental social stability.

THE HEALTHCARE TARGETING MORAL HAZARD

Historically, many ransomware groups maintained informal "ethics" that discouraged targeting healthcare systems due to potential life-threatening consequences. That taboo largely evaporated in 2025, reflecting a concerning evolution in cybercriminal psychology and operational priorities.

Qilin's 71 healthcare victims highlighted a strategic focus on:

- ESXi-driven hospital environments
- 24/7 operational demands
- Legacy clinical systems that are difficult to patch
- Interdependent care-delivery workflows

For attackers, healthcare offers rare leverage: downtime is literally life-and-death, making negotiation pressure immediate.

Government-as-entry point

Warlock's SharePoint-focused campaigns in 2025 showed how collaboration platforms have become efficient entry points into institutional environments. In several cases, adversaries gained access not by breaching sensitive systems directly, but by compromising:

- Internal document repositories
- Workflow hubs
- Inter-agency coordination platforms

This pattern parallels the supply-chain and cloud-service attacks we've seen in state-sponsored operations. This time, they're executed for extortion, rather than geopolitical intelligence. The fallout is nonetheless similar: Loss of operational continuity, undermining of trust and cascading institutional impact.

Exploitation chains and weakness trends

The Vulnerability Exploitation Renaissance

In 2024, Securin identified a clear disconnect between how defenders prioritized vulnerabilities and how ransomware groups actually exploited them. Attackers consistently favored authentication failures, access-control weaknesses and trust-boundary violations – even when those issues ranked lower in standard scoring systems.

IN 2025, THOSE PREFERENCES WERE INDUSTRIALIZED.

Ransomware groups no longer treat vulnerabilities as isolated entry points. They assemble them into deliberate exploitation chains, selecting weaknesses not just for severity, but for how effectively they can collapse trust, persistence and operational control across entire platforms.

The data tells a consistent story.

These CVEs represent the core exploitation patterns our researchers observed across major ransomware campaigns in 2025, spanning collaboration platforms, network infrastructure, virtualization, boot-level trust chains and legacy drivers.

CVES POWERING 2025 RANSOMWARE CAMPAIGNS

Core CVEs and exploitation patterns observed in 2025 ransomware campaigns. These vulnerabilities illustrate a consistent shift toward authentication collapse, platform-scale compromise, and trust-chain abuse across enterprise infrastructure.

CVE	RANSOMWARE ASSOCIATION	FAMILY	AFFECTED PRODUCTS	PRODUCT CATEGORIES	WEAKNESS
CVE-2015-2291	DOGE Big Balls	Fog	intel+ethernet_diagnostics_driver_iqvw32.sys|intel+ethernet_diagnostics_driver_iqvw64.sys|microsoft+windows	Computer Hardware|Desktop Applications|Operating Systems	CWE-20: Improper Input Validation
CVE-2023-27532	Ransom:Linux/Qilin!rfn	Qilin	veeam+veeam_backup_\&_replication	Data Storage & Management| Remote Management| Virtualization	CWE-306: Missing Authentication for Critical Function
CVE-2024-21762	Ransom:Linux/Qilin!rfn	Qilin	fortinet+fortios| fortinet+fortiproxy	Network Devices|Operating Systems|Secure Access|Security Tools	CWE-787: Out-of-bounds Write
CVE-2024-55591	Ransom:Linux/Qilin!rfn	Qilin	fortinet+fortios| fortinet+fortiproxy	Network Devices|Operating Systems|Secure Access|Security Tools	CWE-288: Authentication Bypass Using an Alternate Path or Channel
CVE-2024-55591	SuperBlack	SuperBlack	fortinet+fortios| fortinet+fortiproxy	Network Devices|Operating Systems|Secure Access|Security Tools	CWE-288: Authentication Bypass Using an Alternate Path or Channel

CVE	RANSOMWARE ASSOCIATION	FAMILY	AFFECTED PRODUCTS	PRODUCT CATEGORIES	WEAKNESS
CVE-2024-7344	HybridPetya	Petya	cs-grp+neo_impact|greenware+greenguard|howyar+sysreturn|radix+smart_recovery|sanfong+ez-back_system|signalcomputer+hdd_king|wasay+erecoveryrx	Business Intelligence Software|Computer Hardware|Data Storage & Management|Desktop Applications|Industrial Control Systems|Security Tools	CWE-347: Improper Verification of Cryptographic Signature CWE-426: Untrusted Search Path
CVE-2025-24472	SuperBlack	SuperBlack	fortinet+fortios|fortinet+fortiproxy	Network Devices|Operating Systems|Secure Access|Security Tools	CWE-288: Authentication Bypass Using an Alternate Path or Channel
CVE-2025-49704	4L4MD4R	Mauri870	microsoft+SharePoint_server	Collaboration Platforms|Content Management Systems (CMS)|Data Storage & Management	CWE-94: Improper Control of Generation of Code ('Code Injection')
CVE-2025-49706	Warlock	Warlock	microsoft+SharePoint_enterprise_server|microsoft+SharePoint_server	Collaboration Platforms|Content Management Systems (CMS)|Data Storage & Management	CWE-287: Improper Authentication
CVE-2025-49706	4L4MD4R	Mauri870	microsoft+SharePoint_enterprise_server|microsoft+SharePoint_server	Collaboration Platforms|Content Management Systems (CMS)|Data Storage & Management	CWE-287: Improper Authentication

CVE	RANSOMWARE ASSOCIATION	FAMILY	AFFECTED PRODUCTS	PRODUCT CATEGORIES	WEAKNESS
CVE-2025-53770	Warlock	Warlock	microsoft+SharePoint_server	Collaboration Platforms|Content Management Systems (CMS)|Data Storage & Management	CWE-502: Deserialization of Untrusted Data
CVE-2025-53770	4L4MD4R	Mauri87	microsoft+SharePoint_server	Collaboration Platforms|Content Management Systems (CMS)|Data Storage & Management	CWE-502: Deserialization of Untrusted Data
CVE-2025-53771	4L4MD4R	Mauri870	microsoft+SharePoint_server	Collaboration Platforms|Content Management Systems (CMS)|Data Storage & Management	CWE-287: Improper Authentication
CVE-2025-6264	Warlock	Warlock	rapid7+velociraptor	Collaboration Platforms|Content Management Systems (CMS)|Data Storage & Management	CWE-276: Incorrect Default Permissions CWE-280: Improper Handling of Insufficient Permissions or Privileges

From single CVEs to exploitation chains

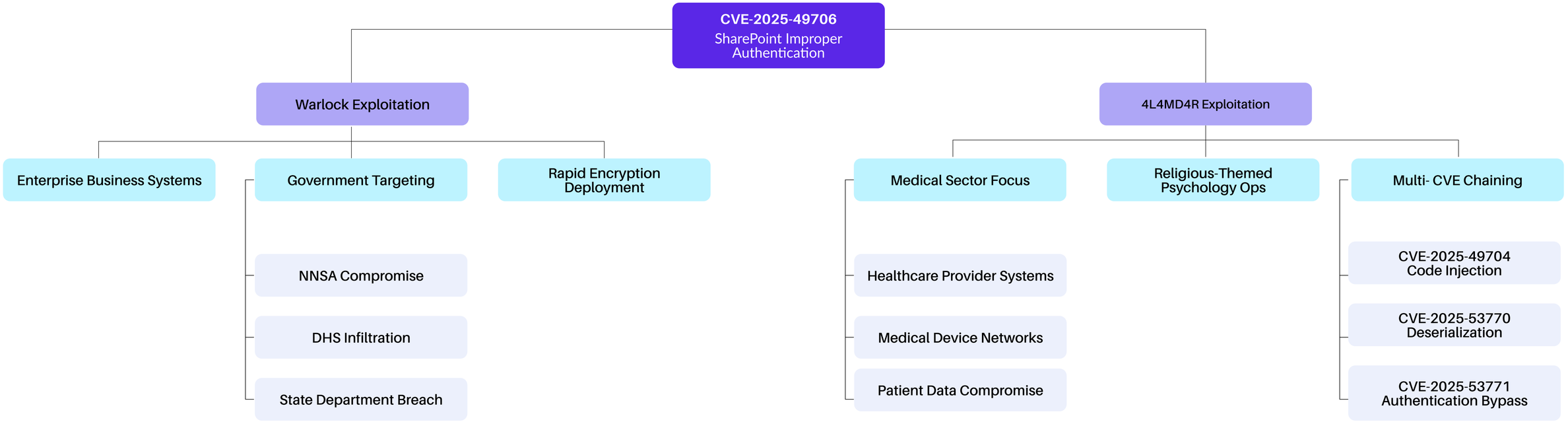
As the table above shows, across ransomware families and campaigns in 2025, several patterns repeat:

- **Authentication bypass and missing authentication**
  (CWE-287, CWE-288, CWE-306)
- **Code execution via unsafe input handling**
  (CWE-94, CWE-502, CWE-20)
- **Trust-chain abuse and persistence mechanisms**
  (CWE-347, CWE-426)
- **Default or inherited permissions failures**
  (CWE-276, CWE-280)

These weaknesses appear again and again across SharePoint, Fortinet, ESXi, UEFI, backup platforms, and even decade-old drivers - not because attackers lack options, but because these flaws scale.

The SharePoint Apocalypse: Collaboration platforms as campaign infrastructure

The emergence of SharePoint-focused vulnerabilities represents one of the most consequential shifts in attack vectors since the proliferation of internet-connected systems. CVE-2025-49706's exploitation by both Warlock and 4L4MD4R groups underlined how collaboration platforms have become the new frontier of cybercriminal activity.



SharePoint's ubiquity across enterprises creates what intelligence analysts describe as a high-value, high-volume target profile. Unlike endpoint compromise, SharePoint exploitation grants access to:

- Internal documentation
- Operational workflows
- Sensitive communications
- Identity-linked collaboration services

Warlock and 4L4MD4R demonstrated how this access can be weaponised at scale. Rather than relying on a single vulnerability, they chained:

Improper Authentication
(CWE-287)

Code Injection
(CWE-94)

Deserialization of Untrusted Data
(CWE-502)

THE RESULT WAS PLATFORM-WIDE COMPROMISE, NOT APPLICATION-LEVEL ACCESS.

Warlock's systematic targeting of U.S. government agencies - including National Nuclear Security Administration (NNSA), National Institutes of Health (NIH), Department of Homeland Security (DHS), and the State Department - signals a significant escalation. While no state sponsorship is claimed, the target selection and tradecraft reflect a level of intelligence alignment rarely seen in traditional ransomware campaigns.

Meanwhile, 4L4MD4R's July 2025 medical-sector intrusion - chaining four SharePoint CVEs in a single campaign - illustrates how vulnerability exploitation has evolved from point attacks to comprehensive platform takeovers. Their chain combining CVE-2025-49706 (Authentication), CVE-2025-49704 (Code Injection), CVE-2025-53770 (Deserialization), and CVE-2025-53771 (Authentication Bypass) represents a masterclass in systematic platform exploitation.

Fortinet’s authentication apocalypse: The network perimeter dissolves

The SuperBlack ransomware group's exploitation of CVE-2024-55591 and CVE-2025-24472 in FortiOS systems represents more than individual attacks - it signals the complete dissolution of traditional network perimeter security models. As such, it represents an attack on foundational trust relationships, not individual services.

Authentication bypass at the network perimeter has cascading consequences:

Segmentation assumptions fail

VPN trust collapses

Downstream security controls become irrelevant.

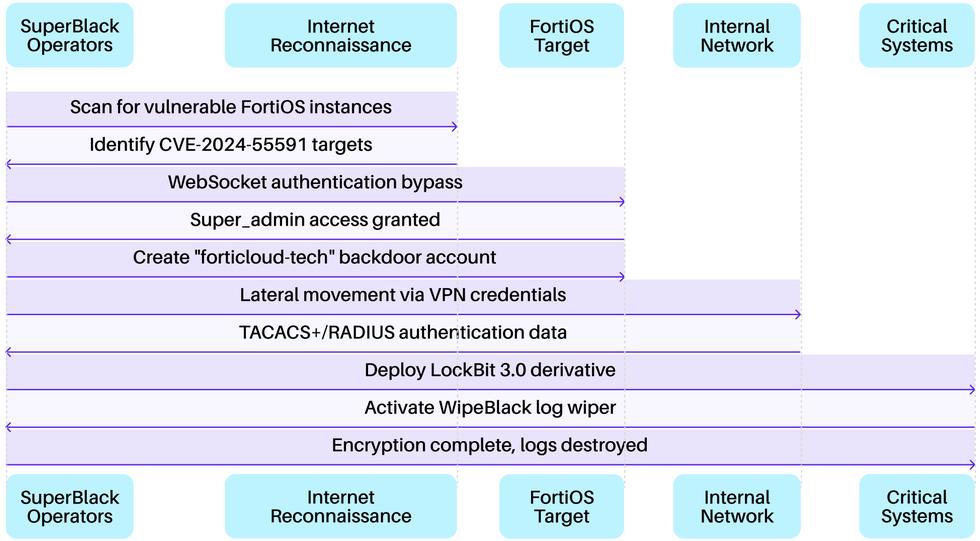
Once firewall authentication is compromised, lateral movement is constrained less by architecture than by attacker intent.

THE MORA_001 CONNECTION

Intelligence analysis suggests SuperBlack’s operator “Mora_001” is a former LockBit insider, representing a new category of threat actor: former ransomware group insiders leveraging insider knowledge to create “next generation” campaigns. The group’s use of LockBit 3.0 derivatives, combined with operational tradecraft mirroring LockBit methodologies, suggests direct lineage from the now-disrupted organization.

BOTTOM LINE

Even as groups are dismantled, tradecraft migrates forward through people, tooling and methodology. This is infrastructure warfare, not application exploitation.



Boot-level persistence: HybridPetya and the UEFI trust chain

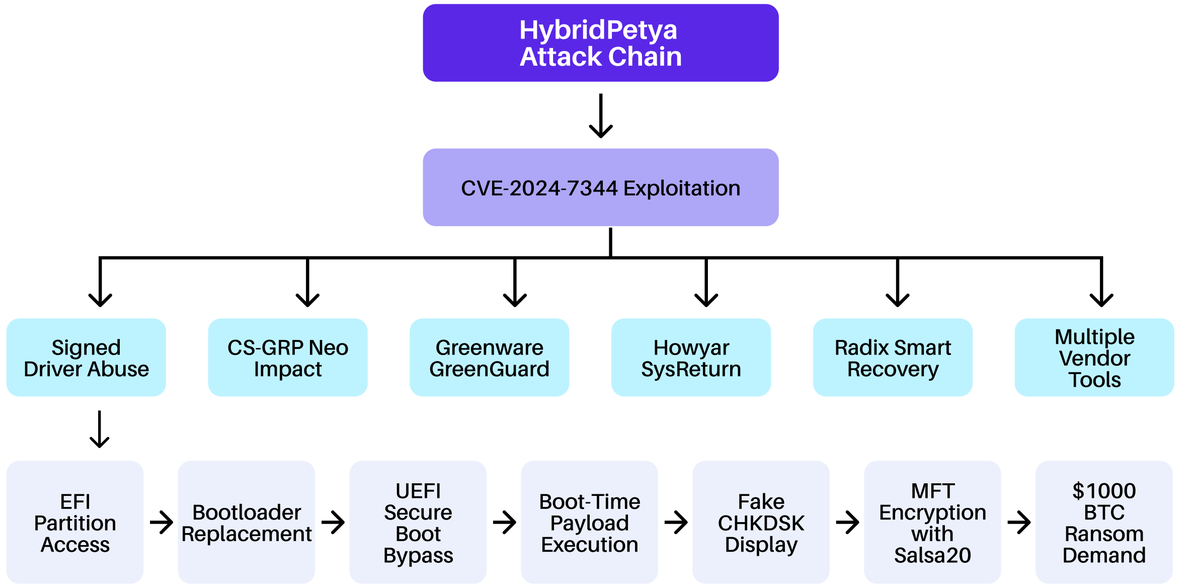
HybridPetya's exploitation of CVE-2024-7344 represents the most technically sophisticated attack vector in the 2025 dataset, marking a clear escalation in how ransomware groups target the foundational layers of system initialization and trust. By abusing signed but vulnerable drivers across multiple vendors, the campaign bypassed Secure Boot protections and embedded persistence below the operating system - an explicit assault on trusted computing models that many organizations still treat as sacrosanct.

This was not simply a boot-level compromise but a weaponisation of the trust chain itself, demonstrating how supply chain relationships can be turned into a delivery mechanism for subverting even the most mature security architectures.

The use of a fake CHKDSK screen during encryption was equally deliberate. While the Master File Table was encrypted in plain sight, victims were conditioned to believe routine disk maintenance was underway, delaying response and neutralising human intervention at the most critical moment. This was psychological control, not theatrics.

BOTTOM LINE

Together, these elements exemplify the new ransomware maturity curve: compromise the system at its roots, manipulate operator perception and control the outcome end to end.



Legacy vulnerability persistence: the CVE-2015-2291 time machine

Perhaps the most uncomfortable finding in our dataset is the continued exploitation of CVE-2015-2291 by the “DOGE Big Balls” ransomware family.

This vulnerability predates modern ransomware by almost a decade - yet remains active in exploitation chains because it persists in production environments.

These “archaeological attack surfaces” exist, not because of technical difficulty, but due to:

- Poor asset visibility
- Inherited driver dependencies
- Broken ownership patching responsibilities
- Accumulated technical debt.

These vulnerabilities persist in production systems despite being well-understood and readily patchable. In 2025, attackers increasingly treat legacy vulnerabilities as low-effort, high-reliability components - especially when paired with modern exploitation techniques.

BOTTOM LINE

Time doesn’t neutralize risk, governance does.

What these attacks taught us in 2025

Across SharePoint, Fortinet, UEFI, backup platforms and legacy drivers, one conclusion is unavoidable:

Ransomware groups are no longer exploiting vulnerabilities - they are orchestrating trust failure.

Each CVE is chosen not for its headline severity, but for how it contributes to:

- Authentication collapse
- Privilege escalation
- Persistent control
- Maximum operational leverage

This shift demands a corresponding change in defence. Patch velocity alone is insufficient. Defenders must understand how weaknesses combine, how platforms interlock and where trust assumptions silently fail.

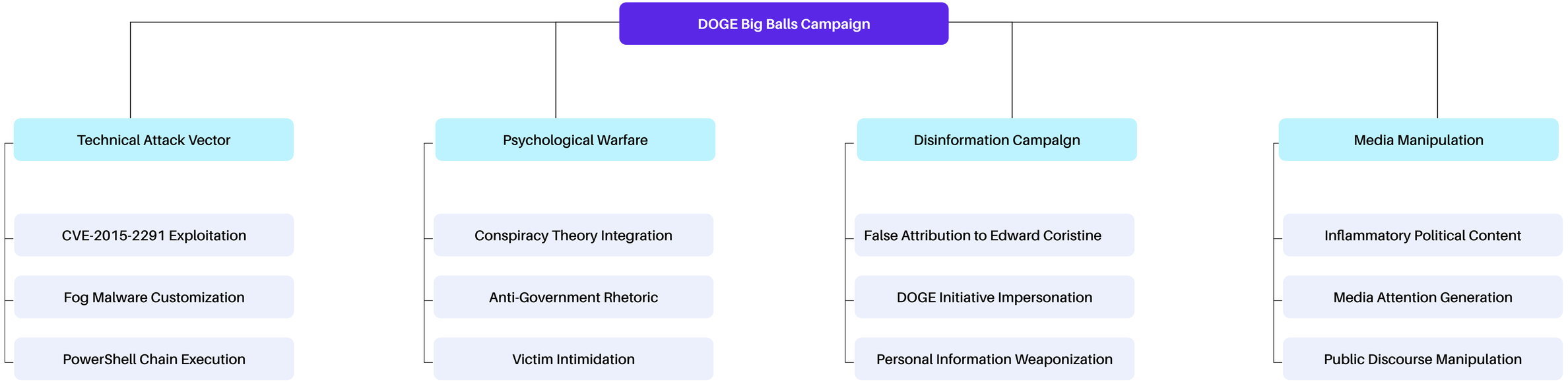
DOGE Big Balls case study

The Psychology of digital warfare - DOGE Big Balls

When ransomware becomes information warfare

The DOGE Big Balls campaign represents a watershed moment in ransomware evolution—the first documented case of ransomware operators integrating comprehensive disinformation campaigns with traditional encryption extortion. This attack doesn't merely demand payment; it weaponizes conspiracy theories, personal harassment and media manipulation to create multi-dimensional pressure on victims and society.

For the first time in our dataset, ransomware operated simultaneously across technical, psychological and political dimensions.



From extortion to narrative manipulation

DOGE Big Balls' operations went far beyond encrypting systems and threatening data leaks. The campaign deliberately weaponised public information and conspiracy narratives to amplify pressure and destabilise response efforts.

Key tactics included:

False attribution of the campaign to Edward Coristine
A government staffer, using publicly available information to construct a plausible but incorrect narrative.

Publication of personal details
Linked to that attribution, exposing an uninvolved individual to reputational harm and potential physical risk.

Conspiracy-laden messaging
Embedded directly into ransom communications, designed to provoke distrust, outrage, and confusion.

This reflects a sophisticated understanding of how media dynamics, political narratives, and personal targeting can act as force multipliers. While DOGE Big Balls presents as a criminal group, its operational psychology closely mirrors influence-oriented campaigns we have previously analysed in DPRK and PRC contexts.

Psychological pressure, attribution fog and the expanded blast radius

Traditional ransomware relies on operational disruption to drive payment.Information-warfare ransomware adds psychological coercion - and deliberately blurs accountability.

By targeting narratives and individuals, not just infrastructure, DOGE Big Balls applied pressure across multiple fronts at once: executive decision-making, legal and regulatory exposure, personal safety considerations, and media amplification. The result was a compressed response window and fragmented authority, forcing victims to manage a cascading crisis that extended well beyond the SOC.

WHEN ATTRIBUTION BECOMES THE WEAPON

A defining feature of this model is attribution fog. When criminal campaigns adopt political narratives, false flags, and identity manipulation, intent becomes opaque in real time. Attribution no longer hinges on declared motive; it must be inferred from behavioural signals - targeting logic, infrastructure choices, and narrative consistency.

This ambiguity is not accidental. It's engineered: designed to slow response, complicate escalation and increase leverage.

The impact extends well beyond the immediate victim. Organizations are forced to coordinate security, legal, communications, and executive leadership under sustained pressure. Public-sector and critical-service institutions face erosion of trust even when claims are demonstrably false. At a societal level, conspiracy-driven targeting chips away at confidence in institutions themselves.

At this point, ransomware is no longer just a cybersecurity problem. It's a governance, resilience and trust challenge.

5 Pillars of modern ransomware

The five pillars of modern ransomware

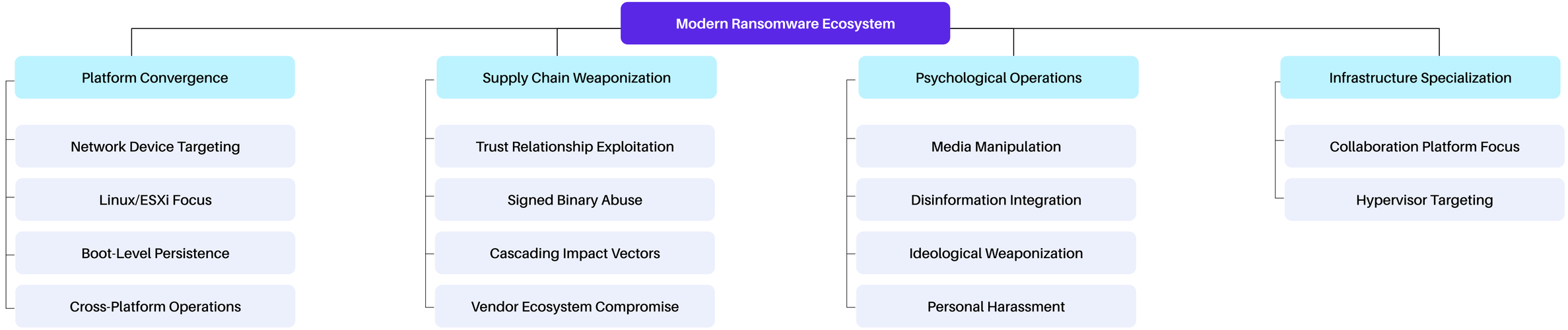
The patterns that defined the 2025 threat landscape

Across the campaigns analysed in this report, ransomware activity in 2025 resolves into a small number of persistent, structural patterns. These patterns cut across groups, tooling, and individual vulnerabilities. They describe not just what attackers did, but how modern ransomware now generates leverage, sustains pressure and converts access into outcomes.

Taken together, these patterns mark a maturation point. Ransomware in 2025 was no longer improvisational or reactive. It is systematic, strategic, and increasingly predictive - shaped by economic incentives, trust relationships and the architecture of modern enterprises.

Securin's analysis identifies five fundamental pillars that now underpin the ransomware threat landscape. These pillars explain why familiar controls continue to fail, why incidents escalate faster and why response feels increasingly constrained. More importantly, they point towards where ransomware is heading next.

As we move into 2026, these pillars are unlikely to fragment or fade. They're more likely to harden - becoming default assumptions for adversaries and baseline conditions for defenders. Understanding them is therefore not an academic exercise. It's a prerequisite for building defensive strategies that can function in the environment that is emerging, not the one we're leaving behind.



The five pillars of modern ransomware

Platform Convergence and Cross-System Exploitation

The traditional Windows-centric view of ransomware has become obsolete. Modern threat actors operate across the entire technology stack, from UEFI boot processes to Linux hypervisors to network appliances. This convergence requires fundamentally different defensive approaches that abandon platform-specific security models in favor of comprehensive ecosystem protection.

PILLAR 1

Supply Chain Weaponization and Trust Exploitation

Multiple campaigns demonstrate systematic exploitation of supply chain relationships and trust boundaries. From signed driver abuse in HybridPetya to SharePoint platform-wide vulnerabilities affecting thousands of organizations, threat actors increasingly view trust relationships as force multipliers rather than obstacles.

PILLAR 2

Psychological Operations and Information Warfare Integration

The emergence of campaigns that blend traditional ransomware with disinformation, harassment, and media manipulation represents a qualitative change in threat actor capabilities and intentions. These campaigns target not just organizational operations but human psychology and social stability.

PILLAR 3

Infrastructure Specialization and Critical System Focus

Rather than targeting endpoint systems, modern ransomware groups increasingly focus on infrastructure components that provide maximum operational leverage—hypervisors, authentication systems, collaboration platforms, and network control planes.

PILLAR 4

Economic Optimization and Strategic Target Selection

The proliferation of ransomware groups paradoxically occurs alongside market consolidation around sophisticated operators who demonstrate superior target selection, attack execution, and revenue optimization capabilities.

PILLAR 5

What it means in 2026

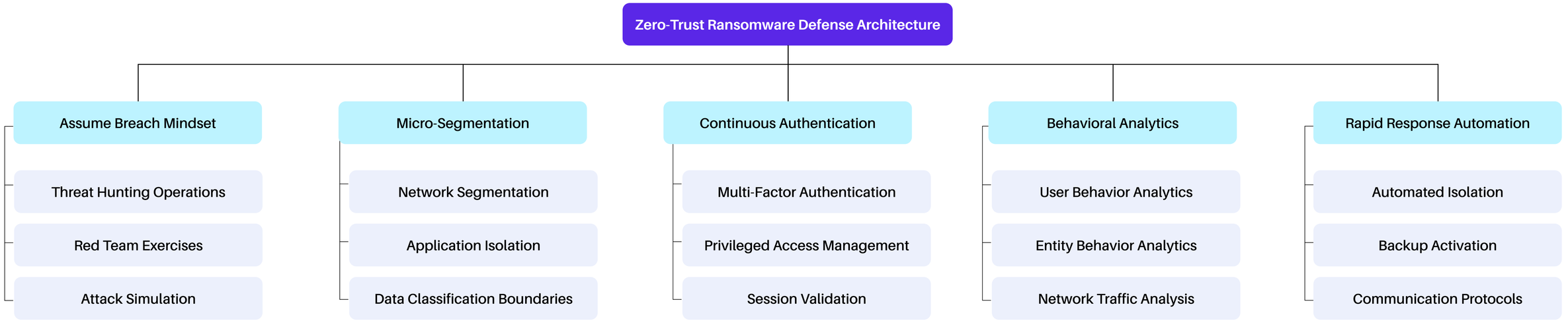
Strategic Defensive Architecture: The Zero-Trust Ransomware Response Model

The five pillars make one conclusion unavoidable: traditional, perimeter-based security models no longer map to how ransomware actually operates.

Modern ransomware assumes breach, abuses trust relationships and applies pressure well beyond the network edge. Defenders must respond in kind.

Securin's analysis points toward a Zero-Trust Ransomware Response Architecture- one that prioritises impact containment over intrusion prevention and resilience over assumed exclusion

In 2026, these pillars are unlikely to fragment or fade. They're more likely to harden - becoming default assumptions for adversaries and baseline conditions for defenders. Understanding them is a prerequisite for building defensive strategies that can function in the environment that's emerging, not the one we're leaving behind.



2026: The path forward

When resilience becomes the strategy

What ransomware demands of defensive strategy in 2026

The 2025 ransomware landscape marks an inflection point. Not because attacks became more frequent, but because they became more intentional. The threats analyzed in this report are no longer just technical problems to be patched or contained. They reflect deeper questions about how organizations, governments, and societies operate under sustained digital pressure.

The ransomware groups active today bear little resemblance to the opportunistic gangs of the past. They operate as resilient, adaptive enterprises - blending criminal efficiency with tradecraft once associated with nation-state actors. Their advantage doesn't come from tools alone. It comes from a clear-eyed understanding of human behaviour, organizational friction and systemic trust failures.

That shift demands a response in kind.

Ransomware is now a pressure strategy, not a malware problem

The target is decision-making and trust, not just systems.

Today's attackers behave like businesses.

They study organizational friction and exploit it with precision and patience.

Better detection on its own won't save you.

Resilience requires identity control, infrastructure hardening and crisis-ready leadership.

Designing for sustained pressure

Defending against modern ransomware requires more than better detection or faster remediation. It requires abandoning outdated assumptions about how attacks unfold, recognising where leverage is really applied and building resilience that spans infrastructure, identity, decision-making, and narrative control. Security can no longer be treated as a perimeter problem. It's now a systems problem.

Ransomware isn't going away, it's evolving - becoming more selective, more coercive and more tightly aligned with the structures it exploits. But that evolution cuts both ways. With rigorous intelligence, clear strategic thinking, and defensive architectures built for reality rather than nostalgia, organizations can shift the balance back.

The choice is no longer abstract. Either defensive models evolve to meet the baseline conditions now in place - or ransomware operators continue to dictate the terms of engagement.

Security is a systems problem now.
Governance and continuity are as critical as firewalls and patches.

Perimeter thinking is obsolete.
Defense in 2026 means designing operations to keep functioning under active attack.

Preparation beats reaction
Organizations that plan for pressure will outlast attackers who depends on panic.

Appendix: Threat actor profiles (AI nexus)

Appendix: Threat actor profiles (AI nexus)

THREAT ACTOR	AI USAGE	PATTERN	SIGNIFICANCE
FunkSec: The Low-Barrier Accelerator	High	AI-assisted malware development and phishing.	Demonstrates how AI lowers the technical barrier to entry, increasing attacker volume and baseline capability.
Global Group The Automation Operator	Moderate	AI chatbots for victim negotiation and workflow automation.	Represents the industrialization of ransomware business operations and scalability.
PromptLock The Adaptive Prototype	Native	Runtime script generation via locally hosted LLM.	Proof-of-concept for polymorphic ransomware that adapts execution per environment.
Qilin The Infrastructure-First Operator	Supportive	AI-assisted phishing localization and reconnaissance.	Uses AI to enhance human tradecraft rather than replace it. Focus remains on hypervisors and infrastructure leverage.

Securin

securin.io

ABOUT SECURIN

Securin is an AI-powered adversarial exposure cybersecurity company revolutionizing the exposure management landscape. By integrating human-augmented adversarial intelligence with comprehensive validation of risks, controls, and remediations, we provide a holistic approach spanning the entire IT environment—including software, cloud, hosting, and AI workloads.