CHECK POINT™

cp<r>
CHECK POINT RESEARCH

Q3
2025

THE RANSOMWARE SECURITY REPORT

Persistent threat, shifting players

TABLE OF CONTENTS:

01 Executive Summary

PERSISTENT THREATS AMID SHIFTING DYNAMICS

Ransomware activity has stayed consistently high throughout Q3 2025, with no sign of real slowing down in sight, despite multiple law enforcement actions earlier in the year. The ecosystem remained active but increasingly fragmented as new and rebranded groups filled gaps left by disrupted operations. At the same time, a few established names resurfaced, signaling how quickly ransomware actors adapt.

KEY FACTS

RECORD-HIGH ACTIVITY CONTINUES:

Ransomware remains one of the most persistent threats, with 1,592 victims posted across leak sites in Q3, despite takedowns.

ESTABLISHED GROUPS REMAIN RESILIENT:

Qilin led activity this quarter while LockBit 5.0 returned in September, quickly recovering from disruption.

AN EXPANDING AND VOLATILE ECOSYSTEM:

With 85 active groups and 14 new entrants, the threat landscape keeps growing, making attribution and defense increasingly complex.

CRITICAL SECTORS UNDER PRESSURE:

Manufacturing and Business Services remain the most targeted as attackers continue to favor sectors that create operational and supply-chain leverage.

POWER SPREADS TO SMALLER ACTORS:

The top 10 groups now account for only 56% of attacks, reflecting a steady shift toward decentralized, short-lived operations.

GLOBAL REACH CONTINUES TO WIDEN:

Ransomware is spreading beyond traditional regions of focus, with South Korea as a new top 10 target.

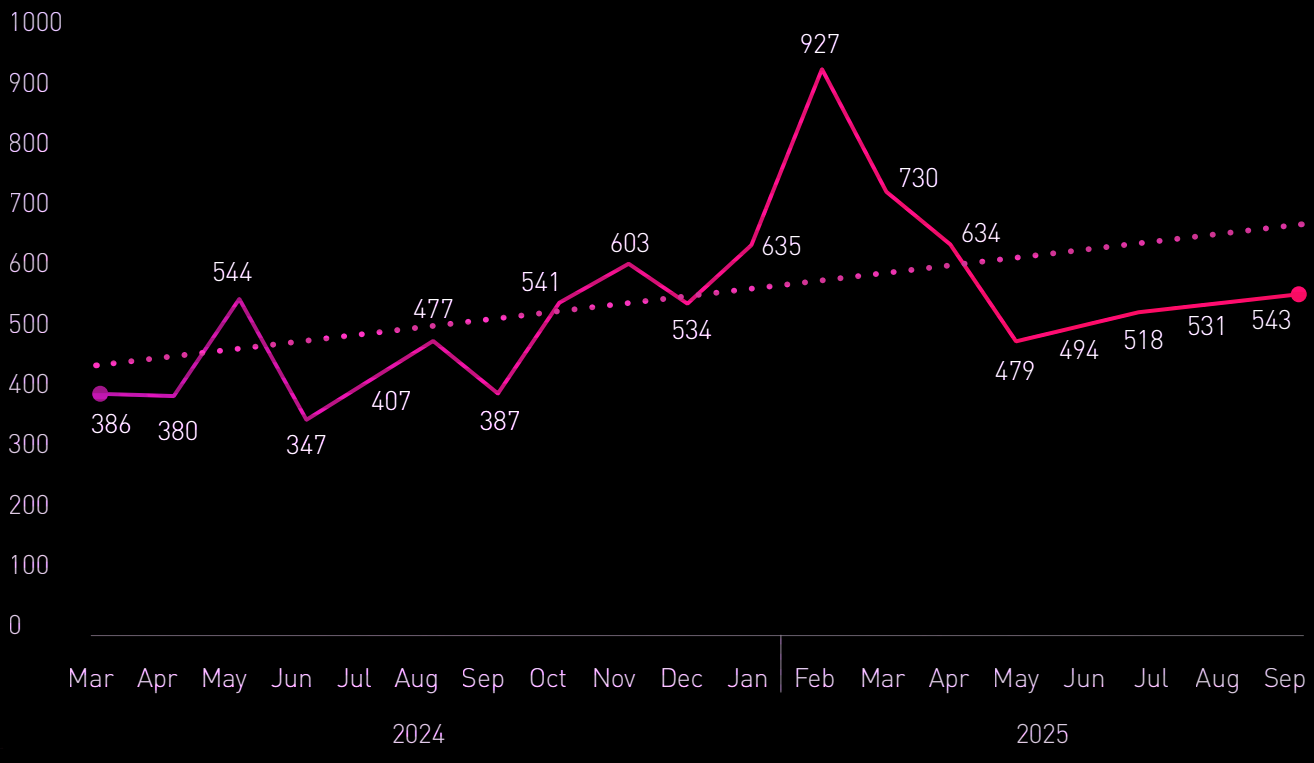


Figure 1. Ransomware activity by month, Q3 2025

02 Ransomware's Fragmented Landscape

SHIFTING ALLIANCES, FLEETING OPERATIONS

The ransomware ecosystem continued to splinter into smaller, short-lived operations in Q3 2025, reflecting an ongoing shift toward decentralization and fluid group structures. Overall attack volumes stayed high, but no single group held dominance. Affiliates shifted between brands, new leak sites rose and fell, and familiar names resurfaced under new identities, keeping the landscape highly active, decentralized, and increasingly unpredictable. This constant churn highlighted the adaptability of ransomware operators, who continue to evolve their methods to maintain relevance and evade law enforcement scrutiny.

KEY DEVELOPMENTS

BRAND FLUIDITY:

Several known actors resurfaced under new names or leak sites, making lineage tracing difficult.

GROUP CHURN:

14 new groups emerged this quarter, many of which are short-term or single-campaign brands.

AFFILIATE PERSISTENCE:

Even after major brand disruptions in Q2, affiliates quickly realigned under other operations, maintaining overall attack volume.

RAAS VOLATILITY:

Frequent tool sharing and code reuse blur group boundaries, complicating response and intelligence efforts.

POWER DIFFUSION:

The top ransomware groups accounted for just over half of all victims in Q3, compared with nearly two-thirds in Q2, underscoring the pace of fragmentation.

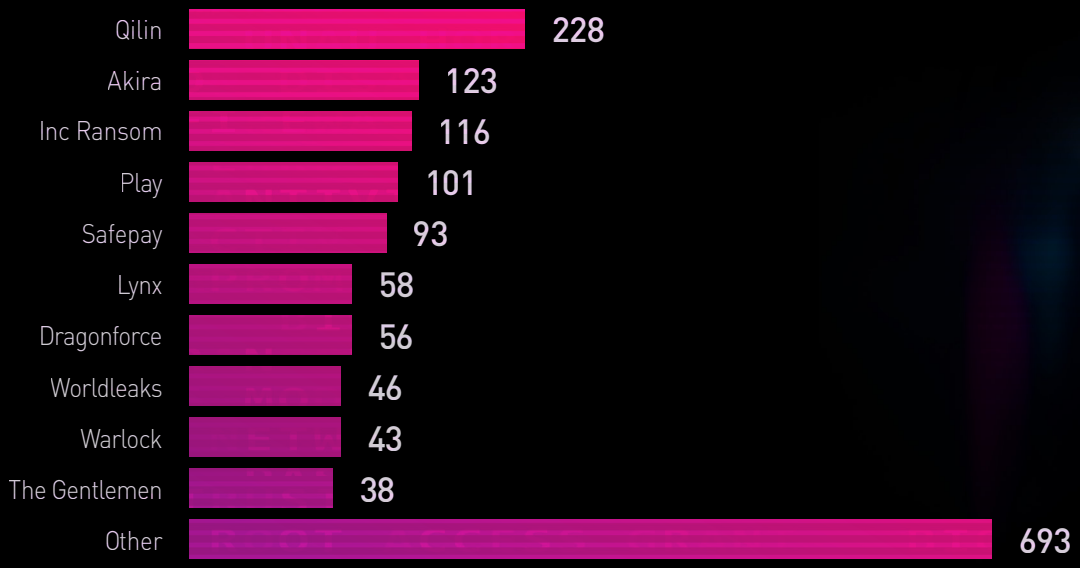


Figure 2 - Share of total victims by top 10 ransomware groups, Q3 2025

03 Threat Actor Highlights

RESURFACING GIANTS AMID FIERCE COMPETITION

Q3 2025 was defined less by sheer attack volume and more by shifting influence among key ransomware groups. A handful of established operations regained momentum, reasserting their presence after periods of relative quiet. Meanwhile, newly formed groups struggled to differentiate themselves in an increasingly saturated and competitive market. This dynamic reflected a maturing ecosystem, where reputation, reliability, and affiliate trust have become just as crucial as technical sophistication in sustaining ransomware operations.

QILIN – LEADING THE QUARTER

Qilin remained the most active ransomware group in Q3 2025, more than doubling its monthly average victim count from around 36 in Q1 to 75 in Q3 - a 108% increase. Its success stems from an open affiliate model that attracts operators across industries and regions, prioritizing volume over selectivity.

We found that Qilin maintains steady infrastructure and frequent leak-site updates, giving affiliates confidence in its reliability. The group also shows unusual brand discipline, at times removing politically sensitive victims to reduce unwanted attention and preserve its reputation.

Technically, Qilin relies on a custom encryptor and well-established exfiltration tools, emphasizing operational consistency over innovation. Together, these factors make Qilin one of the most stable and opportunistic RaaS operations active today.

LOCKBIT 5.0 – BRAND REVIVAL

After months of quiet following enforcement operations, LockBit reappeared in September with a new version– LockBit 5.0. The new version includes enhanced evasion and anti-analysis mechanisms, faster encryption routines, and a randomized 16-character file extension to disrupt signature-based detection. It also incorporates Windows, Linux, and ESXi variants. The new build introduces enhanced evasion and anti-analysis mechanisms, faster encryption routines, and the use of a randomized 16-character file extension to disrupt signature-based detection.

Early victims were reported in the United States, Mexico, Indonesia, and several European countries. LockBit's resurgence shows that if a group's tools and affiliate models remain attractive, even disrupted ransomware groups can re-establish credibility.

```
You have been attacked by LockBit 5.0 - the fastest, most stable and immortal
ransomware since 2019
>>>>> You must pay us.
Tor Browser link where the stolen infortmation will be published:
http://lockbit                                                    .onion
>>>>> What is the guarantee that we won't scam you
We are the oldest extortion gang on the planet and nothing is more important to us
than our reputation. We are not a politically motivated group and want nothing but
financial rewards for our work. If we defraud even one client, other clients will
not pay us. In 5 years, not a single client has been left dissatisfied after making
a deal with us. If you pay the ransom, we will fulfill all the terms we agreed upon
during the negotiation process. Treat this situation simply as a paid training
session for your system administrators, because it was the misconfiguration of your
corporate network that allowed us to attack you. Our pentesting services should be
paid for the same way you pay your system administrators' salaries. You can get more
```

Figure 3 - LockBit 5.0 ransom note from an attack in mid-September 2025

DRAGONFORCE – THE "CARTEL" NARRATIVE

DragonForce continued to promote itself through coalition claims and high-visibility messaging. The group publicly referenced partnerships with Qilin and LockBit , though Check Point Research found no evidence of real collaboration. These claims appear designed to project power and attract affiliates rather than reflect joint operations.

Alongside its media strategy, DragonForce expanded its "data audit" extortion model, which helps affiliates turn stolen information into leverage. Under this approach, an affiliate that steals a large dataset (typically over 300 GB) from a company earning more than US $15 million annually can submit it for review. DragonForce then identifies the most valuable commercial and financial material and drafts a tailored extortion letter to increase pressure on the victim.

Example from Q3: DragonForce reviewed files from a gold mining company, highlighting sensitive financial and contractual data to support its customized ransom demand.

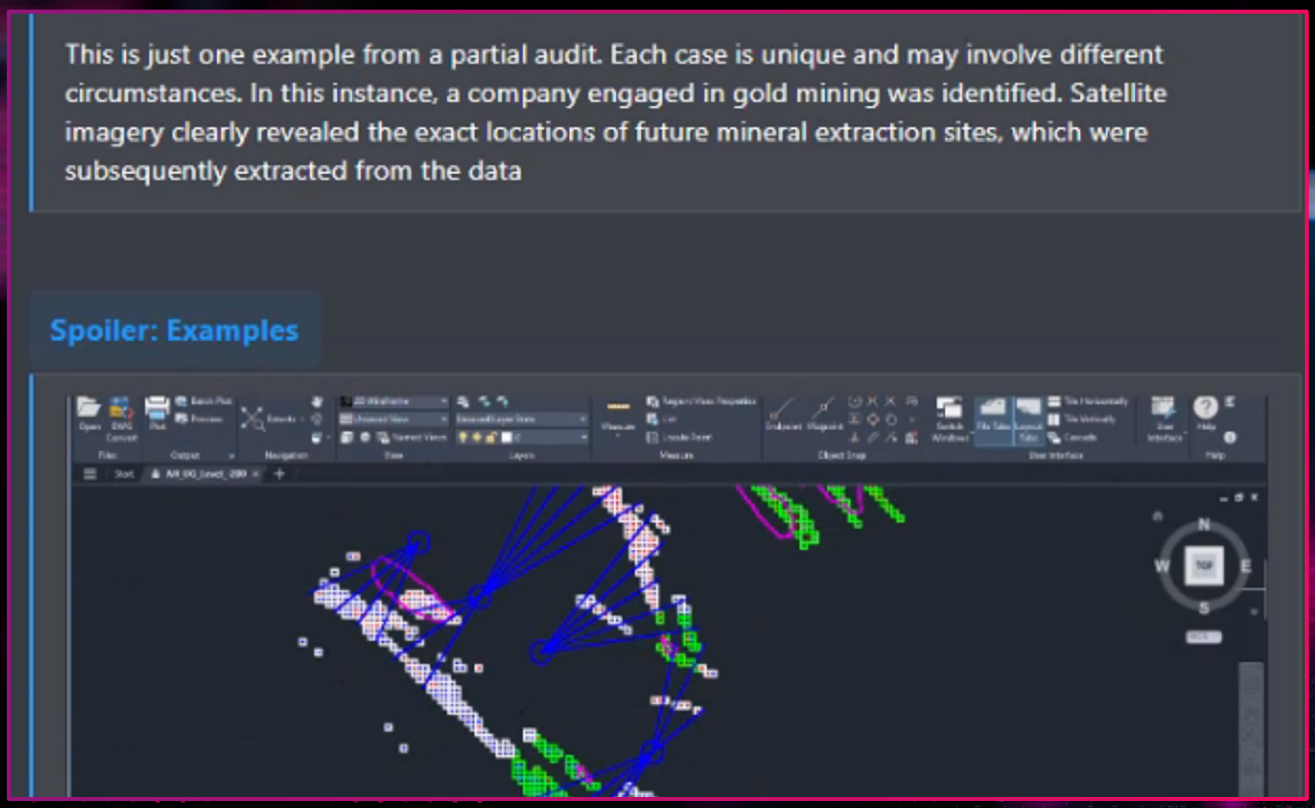


Figure 4 - DragonForce's "data audit" services

D4RK4RMY – RAPID GLOBAL EXPANSION FROM A NEW ENTRANT

First observed on July 7, 2025, d4rk4rmy is a newly emerged ransomware group that quickly expanded, 11 countries, including the US, UK, Brazil, Taiwan, Japan, and South Africa.
The group operates its own data-leak site, publishing victims and negotiation details. Its early targeting shows broad, opportunistic activity across multiple sectors, including education, retail, construction, and technology.

A "Partner Relations" post on the group's leak site indicates that **d4rk4rmy** is **actively seeking collaboration with other established groups and initial-access brokers**, suggesting early ambitions to grow into a **Ransomware-as-a-Service (RaaS)** model.

Figure 5 – d4rk4rmy "Partner Relations" post on its data-leak site, advertising open partnerships with other ransomware groups and access brokers.

d4rk4rmy's speed of operations and geographic reach position it as a rising mid-tier actor amid the increasingly fragmented ransomware ecosystem.

SINOBI – A POSSIBLE REBRAND WITH FAMILIAR TACTICS

First observed in June 2025, Sinobi quickly gained attention for its aggressive operations and professionalized structure. Researchers suspect it may be a rebrand or evolution of the Lynx group, which previously showed operational overlap with INC Ransomware.

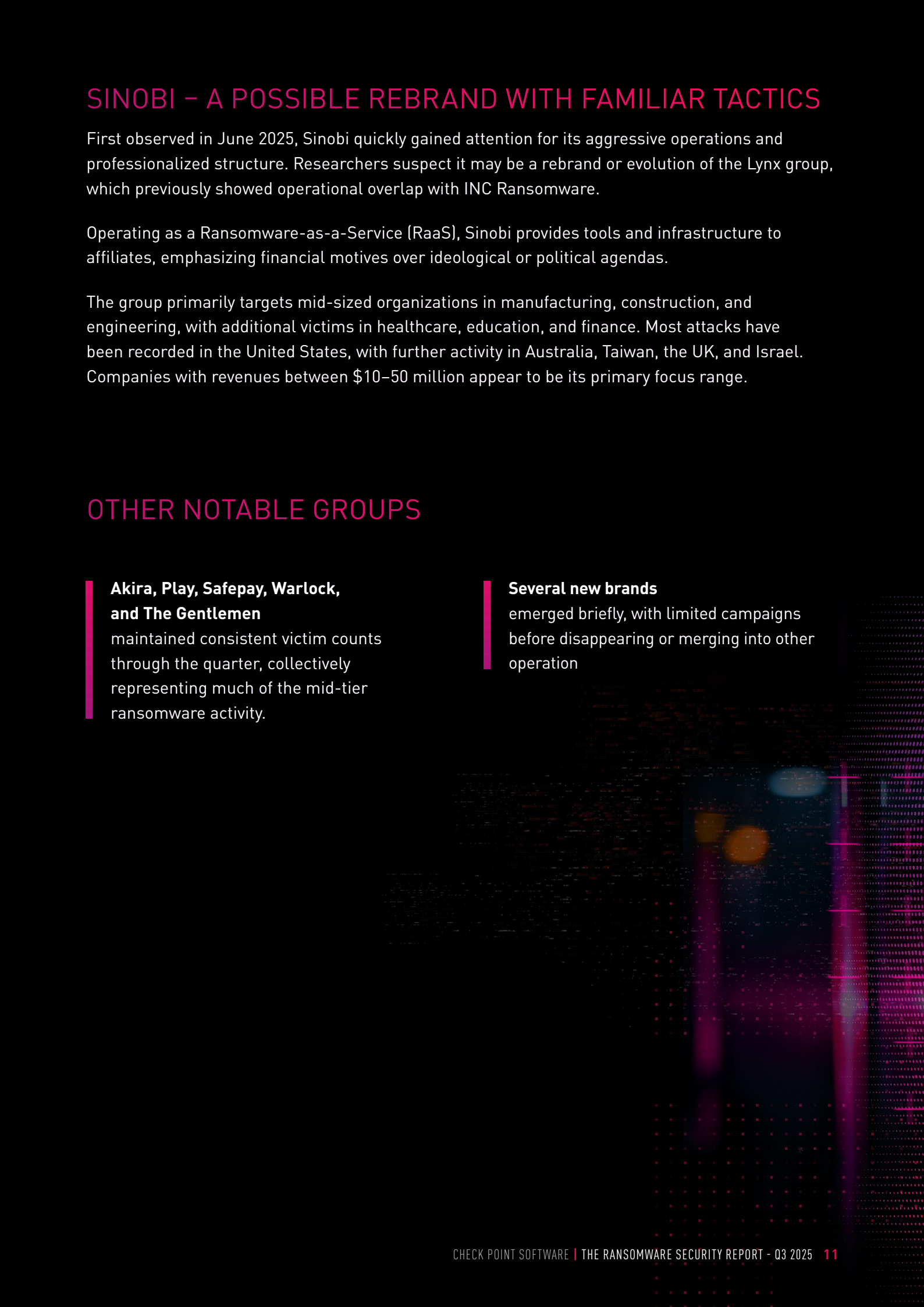
Operating as a Ransomware-as-a-Service (RaaS), Sinobi provides tools and infrastructure to affiliates, emphasizing financial motives over ideological or political agendas.

The group primarily targets mid-sized organizations in manufacturing, construction, and engineering, with additional victims in healthcare, education, and finance. Most attacks have been recorded in the United States, with further activity in Australia, Taiwan, the UK, and Israel. Companies with revenues between $10–50 million appear to be its primary focus range.

OTHER NOTABLE GROUPS

Akira, Play, Safepay, Warlock, and The Gentlemen
maintained consistent victim counts through the quarter, collectively representing much of the mid-tier ransomware activity.

Several new brands
emerged briefly, with limited campaigns before disappearing or merging into other operation



WHAT THIS MEANS FOR CYBER SECURITY PROFESSIONALS

EXPECT RAPID GROUP TURNOVER:

Affiliates can shift between groups within weeks. Maintain visibility on shared TTPs and infrastructure reuse to connect campaigns across group names.

KEEP INTELLIGENCE MAPPING DYNAMIC:

Continuously refresh actor profiles to reflect rebranding and affiliate crossover; static threat cards age quickly in this environment.

PREPARE FOR REVIVED ACTORS:

Disrupted groups may reappear quickly with improved tooling; treat "shutdowns" as temporary setbacks, not conclusions.

04 Geographic and Industry Distribution

REGIONAL HOTSPOTS AND SECTOR TRENDS

Ransomware targeting in Q3 2025 remained heavily concentrated in North America and Western Europe, with new regional spikes in East Asia. Attack distribution reflected both global exposure and sector-specific vulnerabilities. A slight increase was also observed in emerging markets, where weaker defenses continue to attract opportunistic actors. These shifts suggest ransomware groups are gradually diversifying their geographic focus while maintaining pressure on high-value regions.

KEY INSIGHTS

UNITED STATES

Remained the most targeted country, accounting for roughly half of all identified victims. Strong activity also persisted across Western Europe, particularly in Germany and the United Kingdom.

ACROSS INDUSTRIES

Manufacturing and Business Services were most affected, while Healthcare held steady at about 8% of total victims. Other sectors such as Construction, Education, and Retail saw moderate but recurring exposure.

SOUTH KOREA

Entered the top ten for the first time, with most attacks focused on the financial sector.

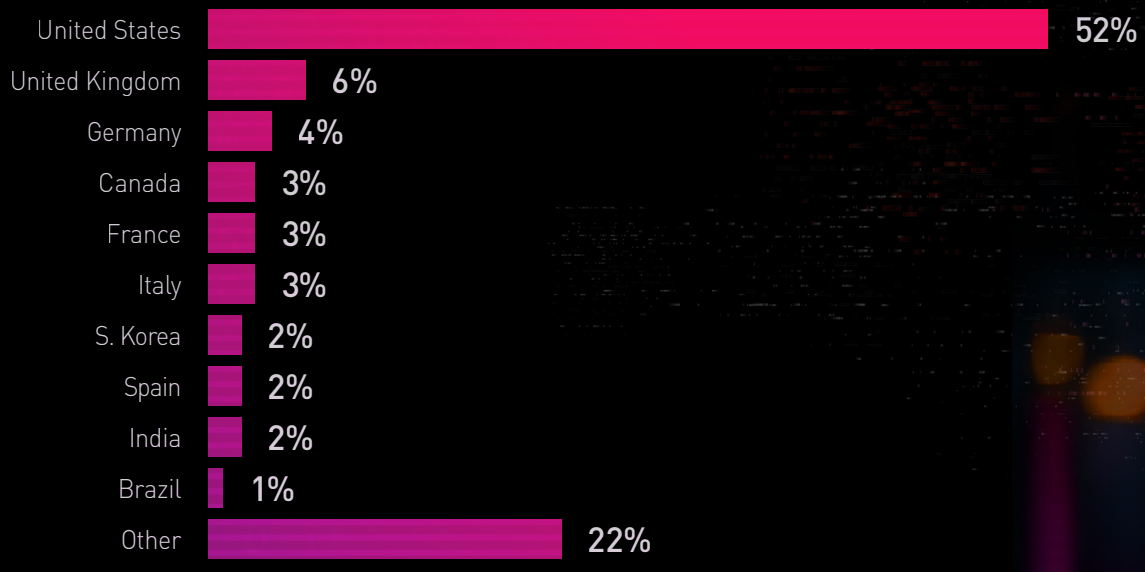


Figure 7 - Top 10 targeted countries by ransomware attacks, Q3 2025

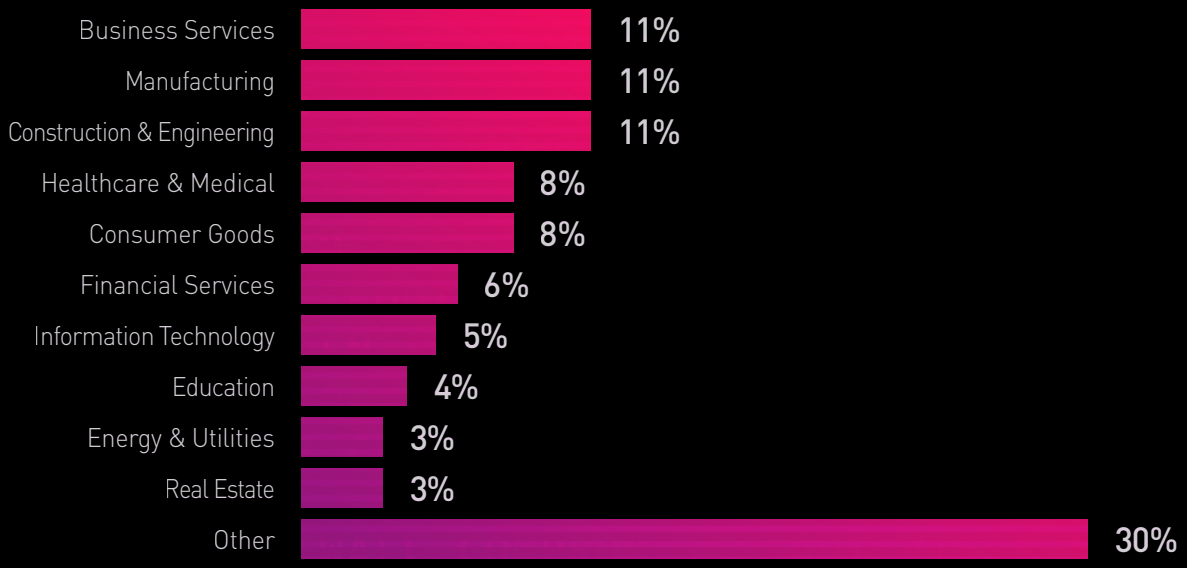


Figure 8 - Victims by industry sector, Q3 2025

WHAT THIS MEANS FOR CYBER SECURITY PROFESSIONALS

EXPAND REGIONAL THREAT MONITORING:

Track evolving activity in East Asia and Europe to anticipate spillover campaigns.

STRENGTHEN THIRD-PARTY OVERSIGHT:

Service providers remain a common vector for ransomware spread; maintain continuous vendor risk assessments.

05 Recommendations and Priorities

BUILDING ADAPTIVE DEFENSES

The trends from Q3 2025 underscore a need for cyber security professionals to strengthen preparedness across technology, people, and processes.

Fragmentation, brand turnover, and fast-moving extortion models demand flexible defense strategies that emphasize detection, coordination, and resilience.

As threat actors adapt their operations with unprecedented speed, organizations must ensure that readiness becomes a continuous, organization-wide discipline rather than a reactive measure.

KEY RECOMMENDATIONS

UNIFY THREAT VISIBILITY:

Integrate telemetry from threat intelligence, endpoint, email, identity, and cloud sources to build a full picture of ransomware behavior across environments.

AUTOMATE FIRST RESPONSE:

Use orchestration and response playbooks to contain lateral movement and isolate compromised assets quickly.

HARDEN DATA PROTECTION:

Segment sensitive data and ensure tested, offline backups that can support restoration under extortion pressure.

REHEARSE INCIDENT COMMUNICATIONS:

Conduct regular tabletop exercises involving security, legal, and communications teams to prepare for data-leak scenarios.

MONITOR FOR COMMON RANSOMWARE ENTRY POINTS:

Track leaked credentials, exposed assets and supplier risk.

EXPAND INTELLIGENCE SHARING:

Participate in industry and regional information-sharing programs to stay ahead of new ransomware variants and tactics.

FOCUS ON RESILIENCE:

Assume compromise is possible; aim to recover business operations rapidly, even when data exposure occurs.

STAYING AHEAD WITH CHECK POINT EXTERNAL RISK MANAGEMENT

Check Point External Risk Management (Formerly Cyberint) reduces risk by helping organizations detect and mitigate external cyber threats before they have an adverse impact. The Check Point External Risk Management solution provides superior visibility through continuous discovery of the evolving attack surface, combined with the automated collection and analysis of vast quantities of intelligence from across the open, deep, and dark web.

A team of global military-grade cyber security experts works alongside customers to rapidly detect, investigate, and disrupt relevant threats before they have the chance to develop into major incidents. Global customers, including Fortune 500 leaders across all major market verticals, rely on Check Point External Risk Management to protect themselves from an array of external risks, including vulnerabilities, misconfigurations, phishing, impersonation attacks, malware infections, exposed credentials, data leaks, fraud, and 3rd party risks.

Together with Check Point's prevention and detection technologies, External Risk Management gives organizations a clearer, more proactive stance against modern ransomware campaigns — helping them spot threats early, manage exposure, and respond before damage escalates. one of the most stable and opportunistic RaaS operations active today.