GUIDEPOINT® SECURITY

Ransomware and Cyber Threat Insights

A GRIT Report

Q1 2026
January-March 2026

Contents

Methodology

Data collected for this report was obtained from publicly available resources, including threat groups themselves. It has not been validated by alleged victims. Collected data is reviewed for potential duplications or inaccuracies and are adjusted accordingly. Thus, the number of publicly observed attacks and the actual number of attacks conducted may not be equal. Some groups do not publicize all of their victims, and almost all groups offer an option to withhold announcement if the victim pays a ransom within a specified timeframe and/or remove the victims once a ransom has been paid. Additionally, some groups include incomplete information about their victim or claim an attack despite successfully attacking only a small subset of their target. For these reasons, the data in this report is useful in aggregate, but should be evaluated as a report consisting of data sources that have variability. Despite the variability, this report is still an accurate representation of the total ransomware threat landscape.

We note that this report includes data and analysis of several groups that may be better described as "extortion" groups rather than "ransomware" groups. These groups may eschew encryption and instead focus only on data exfiltration and extortion, or may not perform intrusion operations of any kind, instead extorting or re-extorting organizations based on historically compromised data. While these groups do not deploy ransomware, we are including them in our reporting due to their relationships with other ransomware groups and their impact on the extortion-based cybercrime environment.

Finally, we make efforts to exclude from our data those groups which self-identify as "hacktivists", compromised data brokers and markets, or non-financially motivated data thieves and leakers. While these actors and venues doubtlessly have impact, we distinguish them from financially-motivated cybercrime and data extortion, which is the primary focus of this report. For this reason, our data may periodically reflect lower total numbers of incidents than other, similar public reports.

Quarterly Ransomware Summary

The first quarter of 2026 saw a consistent volume of ransomware activity relative to both Q4 2025 (quarter-over-quarter (QoQ)) and Q1 2025 (year-over-year (YoY)). After a spike in activity to end 2025, victim numbers have remained level, neither increasing nor decreasing substantially. The number of active groups operating also remained steady QoQ and YoY.

This quarter also saw a slight reordering in the most active ransomware groups observed, with The Gentlemen rising to become the second most active group based on their public claims of 182 distinct victims. This marks a stark increase in operational activity for the group, which claimed only 35 victims and placed 16th in Q4 2025. Conversely, we observed decreased operational activity from prior frontrunners, Qilin and Akira. Although Qilin remained the most active observed group with 361 victims, this still reflected a 25% decrease from its peak of 484 victims in Q4 2025. Akira's observed activity similarly declined from 226 in Q4 2025 to 176 in Q1 2026, a 22% decrease. This decrease in Akira's observed activity is likely a result of outlier performances in Q3 and Q4 2025 attributed to exploitation of vulnerabilities in SonicWall SSLVPN appliances.

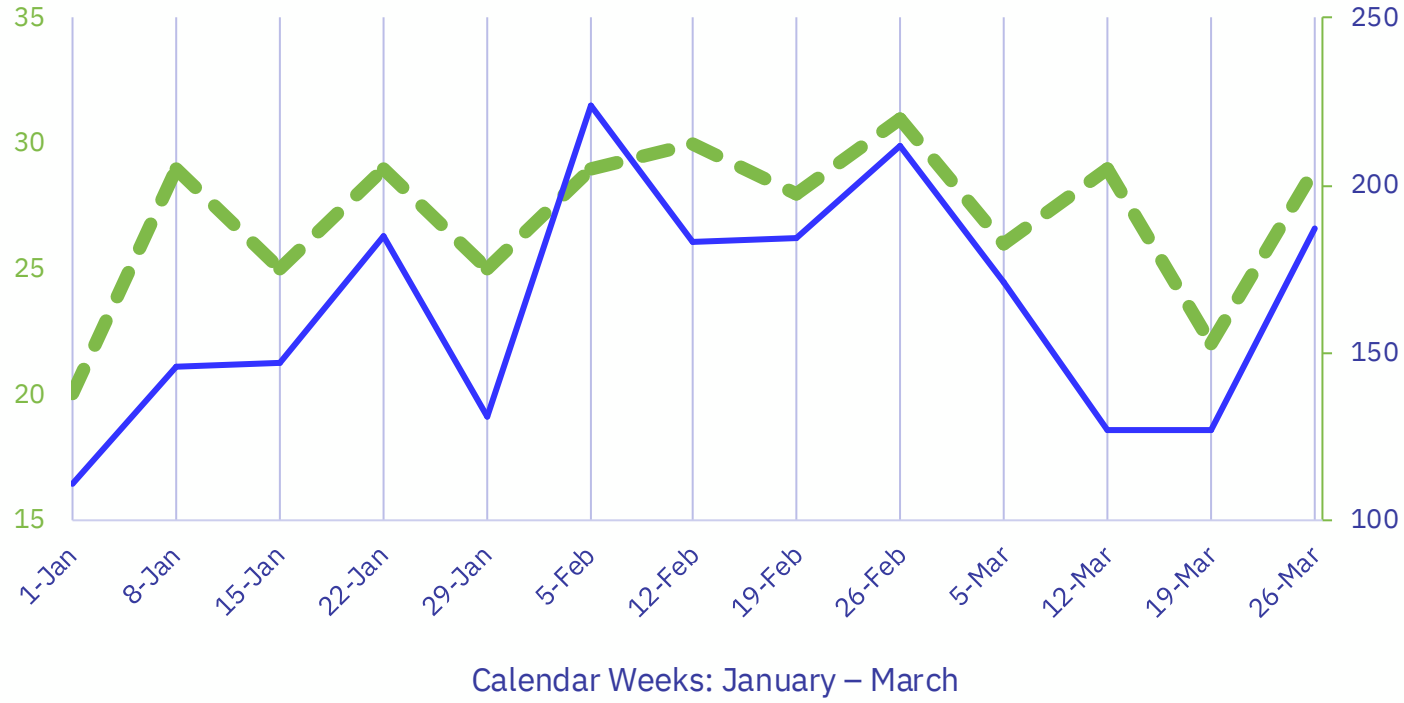
Additionally, we continued to see the effects of Clop's (aka Cl0p) Oracle E-Business Suite mass exploitation campaign. The group continued to claim victims in Q1 2026, despite the exfiltration having occurred during the later months of 2025. This continues Clop's historical habit of drawing out victim posts for several months after mass extortion campaigns.

While this quarter's ransomware activity remained consistent, the overall cyber threat landscape remained anything but. Kinetic operations in the middle east have led to increased cyber operations attributed to Iran-aligned "hacktivist" groups, including Handala. Although the impacts from these operations have, in some cases, been exaggerated, we explore their fallout and ties to the Iranian state in this quarter's report.

	Q1 2026	Q4 2025	Q1 2025
Total Publicly Posted Ransomware Victims	2,135	2,287	2,063
Active Ransomware Groups	68	69	69
Average Daily Victims	23.7	24.9	22.9

Threat Actor Trends

Rate of Publicly Posted Ransomware Victims, Q1 2026



Total Posts	Total Groups	Average Posts per Week	Average Groups Posting per Week
2,135	**68**	**164**	**27**

The first quarter of 2026 saw mostly steady operational activity throughout the months of January, February, and March, with new victim post rates observed at a rate of approximately 150-200 victims per week throughout. As is typical, we observed a “slow start” to the year, a recurring annual trend we typically attribute to observance of Orthodox Christmas in early January across eastern Europe, from where many ransomware affiliates operate. GRIT has observed this decline in ransomware activity during the first weeks of January each year since 2023.

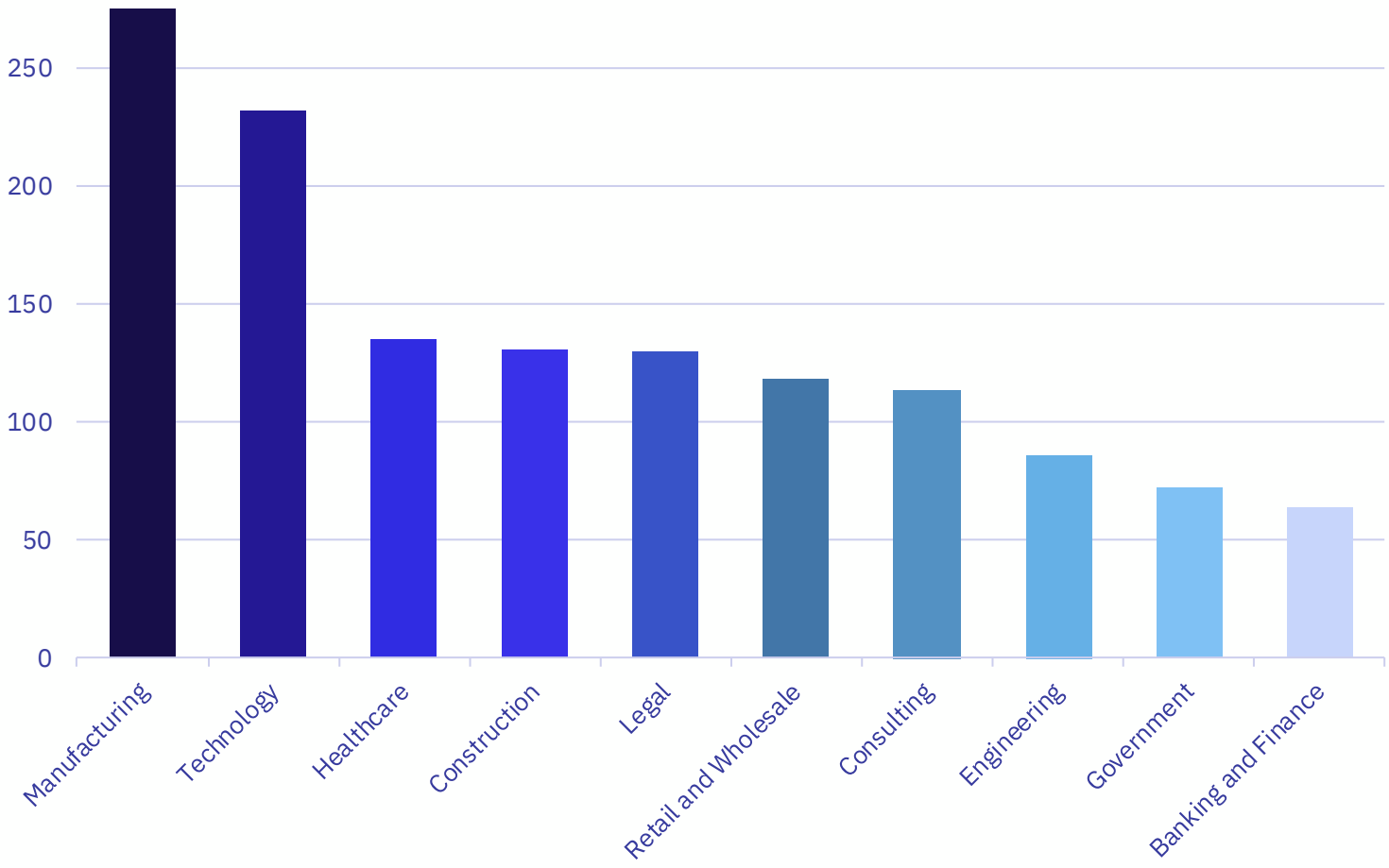
We observed a small spike in activity at the outset of February, which was driven by Clop claiming 54 victims in a single day. The victims were likely claimed as a result of Clop’s Oracle E-Business Suite mass extortion campaign, which began in Q4 2025.

GRIT noticed a slight decline in observed victims of Qilin and Akira, typically the most prolific ransomware groups, which dropped by 25% and 22% QoQ, respectively. This decrease in observed activity is responsible for reduced activity overall and can be attributed to outsized operational performance by the groups tied to vulnerability exploitation campaigns in late 2025.

Most Impacted Industries, Q1 2026

The Gentlemen's notable increase in operations led to their presence in the "Top 3" for several industries for the first time. It stands out given their recent emergence in the ransomware ecosystem in 2H of 2025. This outsized performance early on could indicate that the group's core administrators or affiliates bring experience from other Ransomware-as-a-Service groups, bringing a kick-start to the group's operations.

Manufacturing remains the most impacted industry, where it has remained for over a year. Healthcare saw disproportionate impacts from newer groups Insomnia and Genesis, along with Qilin, though all other industries saw their highest impacts stemming from "the usual players" – Qilin, Akira, Play, Clop, and INC.



Manufacturing
- Qilin
- Akira
- The Gentlemen

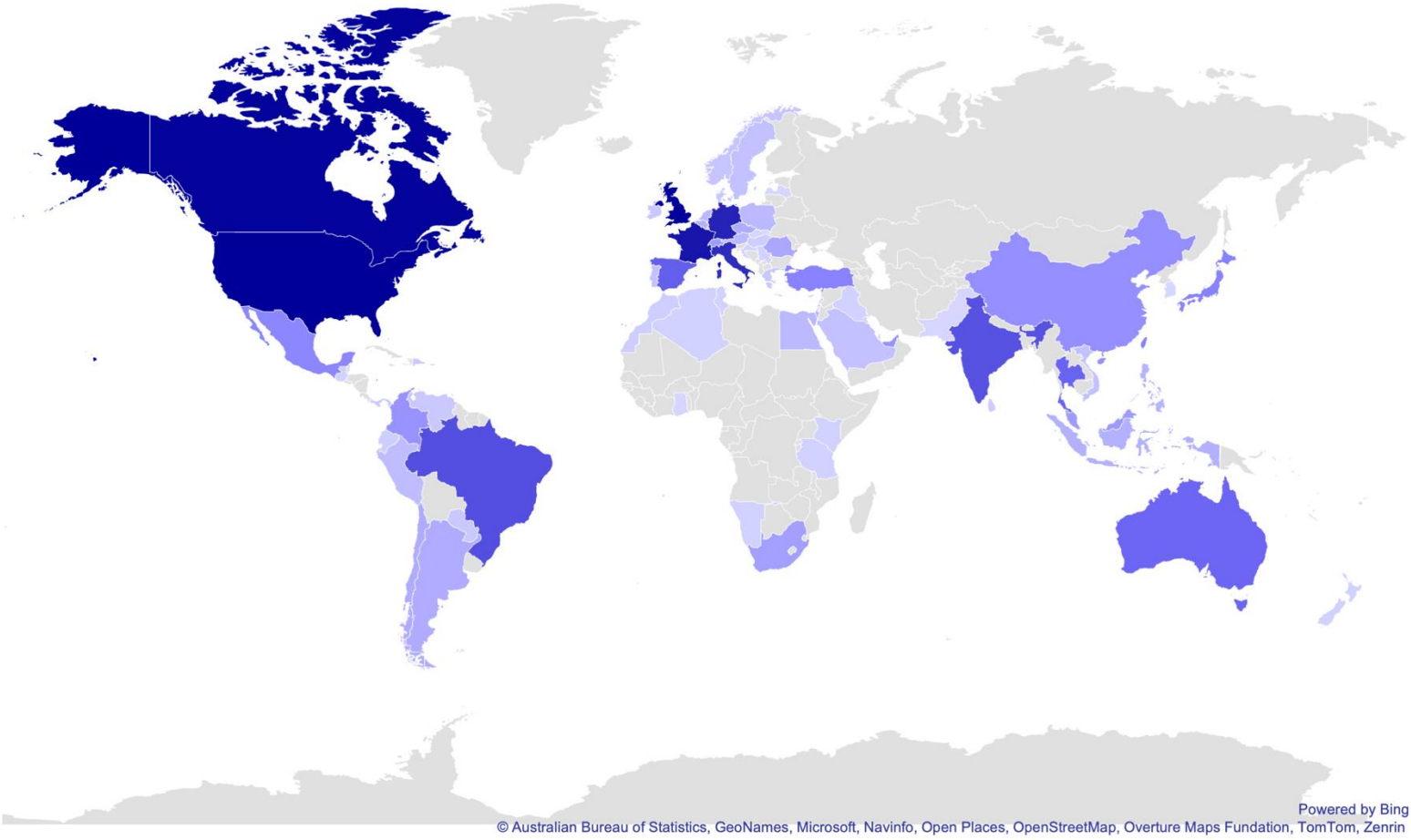
Technology
- Qilin
- Clop
- The Gentlemen

Healthcare
- Qilin
- Insomnia
- Genesis

Construction
- Qilin
- Play
- Akira

Legal
- INC Ransom
- Akira
- Clop

Geographic Breakdown of Ransomware Victims, Q1 2026



Top 10:

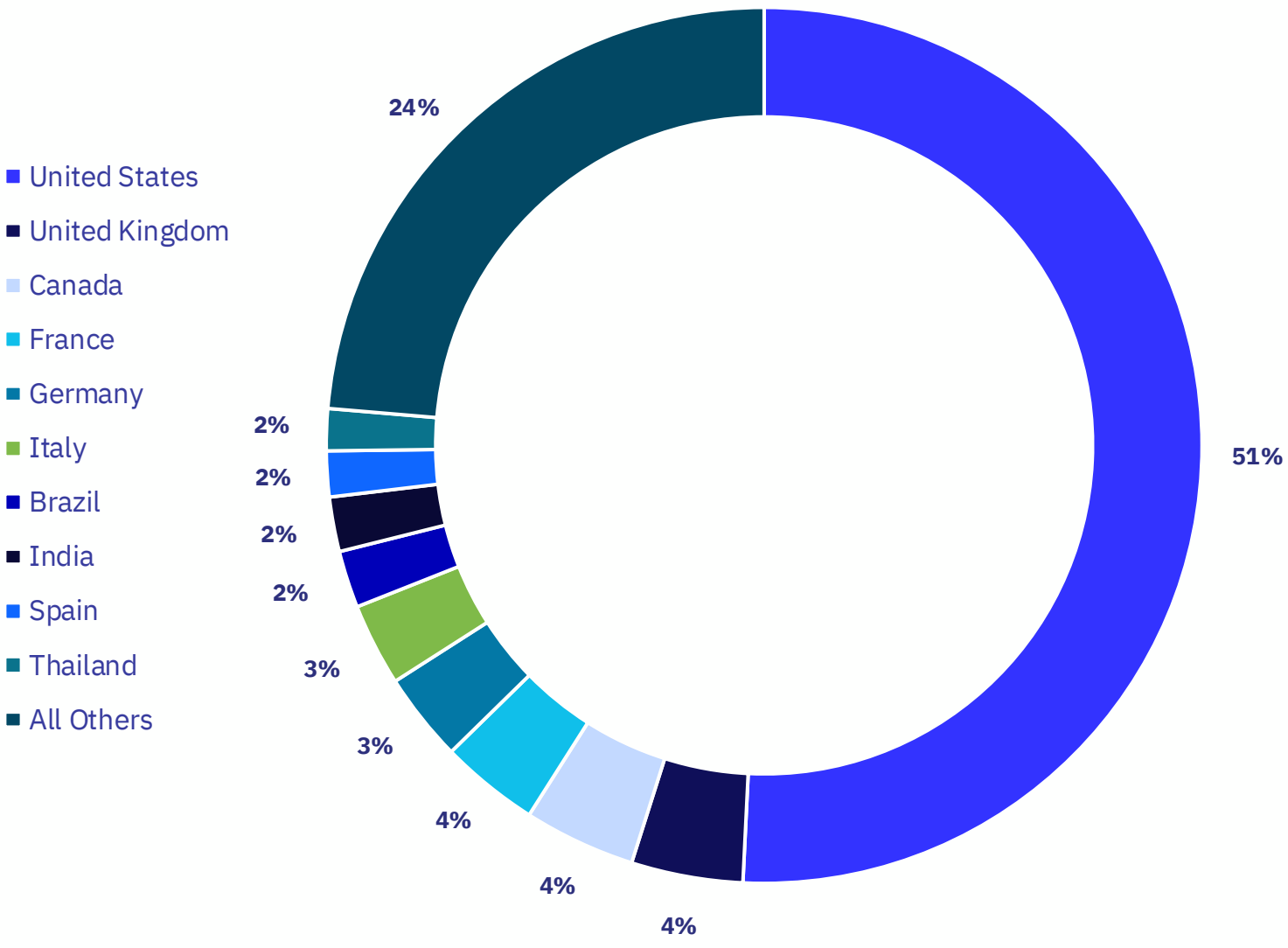
1. United States (1084 | 50.77%)
2. United Kingdom (88 | 4.12%)
3. Canada (88 | 4.12%)
4. France (78 | 3.65%)
5. Germany (70 | 3.28%)
6. Italy (65 | 3.05%)
7. Brazil (45 | 2.11%)
8. India (43 | 2.01%)
9. Spain (36 | 1.69%)
10. Thailand (33 | 1.55%)

Ransomware Impacts by Country, Q1 2026

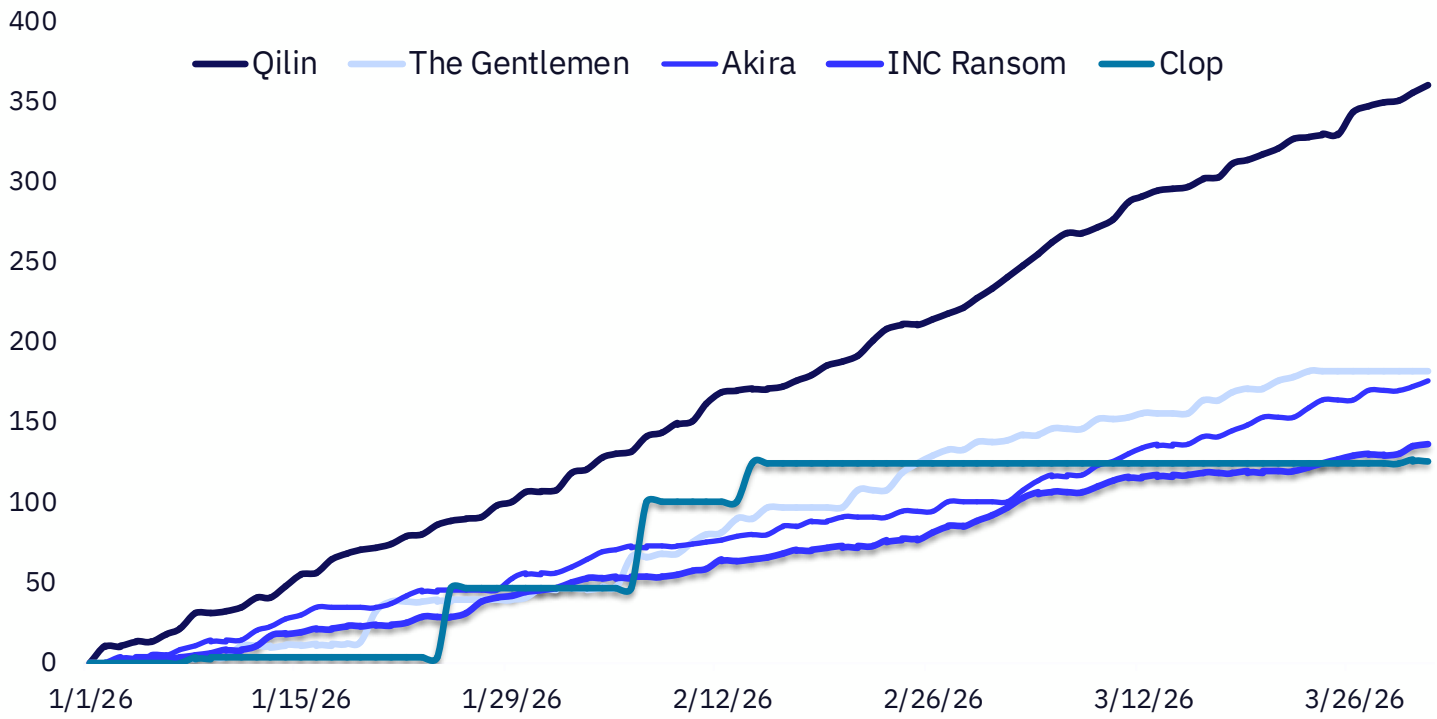
The United States remains, unsurprisingly, the most impacted country in Q1 2026. Similarly, frequently targeted western nations – the United Kingdom, Canada, France, Germany, and Italy – occupy the next five highest spots.

Thailand entered the top 10 for the first time since we began tracking victim data in 2022, indicating an increased level of ransomware impacts in another developing economy.

Brazil and India remain consistent towards the bottom of the top 10, reflecting continued operational impacts against these developing economies.



Cumulative Victims by Threat Group



Qilin

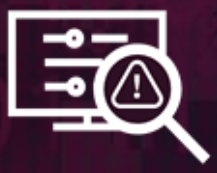
Qilin, which first appeared in 2024, rose to much greater prominence by the end of 2025 by publicly claiming the highest number of victims amongst all ransomware groups we observed. While Qilin's open recruitment model for affiliates likely allows the group's affiliates to attack in greater numbers, it suffers from higher rates of non-payment relative to payment when compared to other ransomware groups, including Akira. As a result, while Qilin remains the most prolific group by observed victim volume, they are far from the most "profitable."

The Gentlemen

The Gentlemen, a relative newcomer to the ransomware ecosystem, first appeared in second half of 2025. They rose quickly to claim the second highest number of victims in Q1 2026 after an unimpressive early performance in Q4 2025. While The Gentlemen may be a newer group, this pattern of rapid growth very likely indicates the participation of experienced affiliates and operators behind the moniker.

Akira

Akira is one of the longest-operating RaaS groups among current active ransomware operations, having first emerged in 2023. Akira had its most "successful" quarter of ransomware in Q4 2025. The group was unable to match it in Q1 2026. Akira's victim count from Q4 2025 (226) dropped 22% in Q1 2026 to 176 victims, likely reflecting the declining utility or efficacy of exploiting SonicWall SSLVPN vulnerabilities its affiliates depended upon in late 2025.



Threat Actor Spotlight: NightSpire

Threat Actor Spotlight: NightSpire

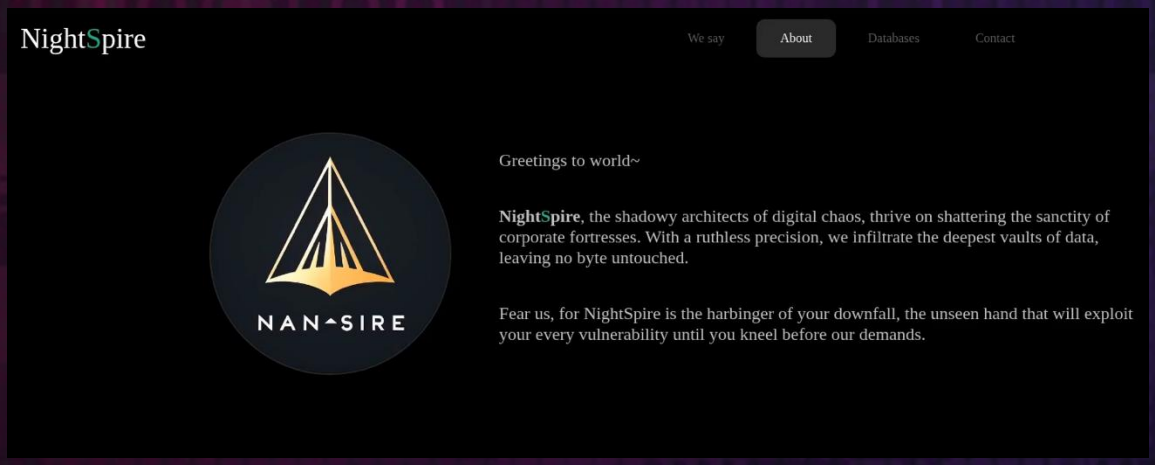
NightSpire is a financially-motivated ransomware group focused on data theft and extortion. Since emerging in 2025, it has rapidly established itself as one of the more aggressive and prolific actors in the current threat landscape. In just over a year of operations, the group has recorded 175 victims across 28 industries – posting 74 on its data leak site (DLS) in Q1 2026 alone. NightSpire is believed to be an insular group, conducting operations in-house, a notable departure from the more common affiliate-based Ransomware-as-a-Service (RaaS) model that dominates the ransomware ecosystem. This structure limits the group's exposure but also constrains operational scale.

A logo used by the NightSpire ransomware group
Source: Ransomlook

NightSpire's targeting is broadly opportunistic rather than sector specific. The group targets organizations with exposed external assets and weak security postures, regardless of industry. That said, there are clear patterns in the group's observed victims. NightSpire's attacks are concentrated in the United States, accounting for over 40% of its victims, with a secondary concentration across Western Europe, Asia, the Middle East, and Africa. Analysis of known victims reveals that the most frequently attacked industries include manufacturing, technology, and construction.

Threat Actor Spotlight: NightSpire

NightSpire has been observed gaining initial access through CVE-2024-55591, which is a critical authentication bypass vulnerability affecting certain versions of FortiOS and FortiProxy. By making these requests, an unauthenticated attacker can gain super-admin privileges and obtain full control of the device without valid credentials. Fortinet disclosed the flaw on January 14, 2025, by which point hundreds of thousands of internet-facing devices had been exposed. Secondary access vectors include RDP brute force and phishing campaigns. These behaviors reflect larger trends across ransomware operations which GRIT classifies as "Developing". Groups in this category often rely on traditional access methodology, rather than novel attack patterns.



NightSpire's "About" Page

Once inside the network, NightSpire moves laterally using legitimate tools such as PowerShell, PsExec, and Windows Management Instrumentation (WMI). All of these are living-off-the-land (LotL) techniques that help avoid early detection. The group escalates privileges, dumps credentials, and maps out environments to gain control over key systems. The group's DLS acts as both a threat and a negotiation platform, with communications facilitated via encrypted channels. Of note, once the countdown timer expires on NightSpire's DLS, the group posts the data for "sale", but it does not provide a specific way to download or purchase the data. Inconsistencies like this are common indicators of Developing groups, which tend not to have streamlined operations like those of more Established outfits.

NightSpire represents a credible and sustained threat, particularly for small- and medium-sized businesses (SMBs) with unpatched perimeter infrastructure. The group has demonstrated remarkable operational consistency since March 2025, with a total victim count confirming significant scale. As with many ransomware operators, proactive patching, behavioral monitoring, and incident response planning are essential countermeasures against this threat.

Threat Actor Spotlight: NightSpire Mitigations and Detections

Mitigations:

- Restrict unauthorized VPN and RDP access by requiring MFA on all remote services and limiting access to known IP addresses or approved devices
- Patch CVE-2024-55591 (FortiOS/FortiProxy Authentication Bypass)
- Install EDR tools on all workstations and servers
- Restrict and Monitor Remote Access Tooling, including Chrome Remote Desktop, AnyDesk, or similar RMMs

Detections:

- Monitor and restrict the execution of PowerShell, PsExec, WinSCP, and megaCMD via application controls (AppLocker/WDAC) for non-approved user groups.
- Monitor and restrict cloud exfiltration channels , such as MEGA

Industry Spotlight: Construction

Industry Spotlight: Construction

The construction sector is an attractive ransomware target due to a convergence of operational and structural vulnerabilities. There were a recorded 131 ransomware victims in Q1 2026. This represents a 12% increase from Q4 2025 (117 victims) and a 44% YoY increase from Q1 2025 (91 victims). Construction advanced from sixth to fourth in GRIT's industry rankings, trailing only manufacturing, technology, and healthcare. This growth is notable against a broader trend of declining ransomware victims QoQ. Construction was among the few sectors to move in the opposite direction.

Operationally, the construction sector is highly sensitive to disruption, as halted work can trigger contract penalties, damage client relationships, and jeopardize future bids. Construction firms present a reliably exploitable attack surface. Project documentation like blueprints, engineering drawings, subcontractor bids, RFIs, and change orders all carry independent extortion value beyond the impact of encryption alone. Specialty contractors routinely maintain connectivity to client and general contractor networks, meaning a single compromise can produce lateral exposure across multiple organizations. In Q1 2026, GRIT observed a victim whose leaked data explicitly referenced federal defense project work, illustrating how a mid-sized contractor's compromise can surface government-adjacent documentation with legal and national security implications.

Industry Spotlight: Construction

When operations are disrupted, the pressure to restore function quickly and protect existing and future contracts creates a strong incentive to pay ransoms. The nature of construction firms' IT and information security posture compounds this risk considerably. Unlike industries where technology is core to the business model, construction firms are more operationally focused. In other words, revenue is generated on job sites and through operational efficiency, not server rooms or technological advancements. This means that at the infrastructure level, cybersecurity investment often lags throughout the sector, with many firms running legacy infrastructure and limited detection capabilities. IT and cybersecurity investment frequently compete with equipment, labor, and materials for already constrained budgets and rarely wins in many firms.

At many small- and mid-sized contractors, cybersecurity investment is hindered by a lack of regulatory pressure and limited direct exposure to cyber incidents. Both of these issues have driven maturity in industries like healthcare and financial services. Dedicated security personnel and enterprise tooling are difficult to justify in this environment. Most firms rely on MSPs or third-party IT support, which can introduce risk when providers are not held to consistent standards. The result is an infrastructure profile characterized by unpatched legacy systems, permissive remote access configurations, and absent or untested incident response capabilities. For ransomware operators, this profile is a known quantity. Industries where unmanaged endpoints, consumer-grade VPN products, and no dedicated security function are common represent a target-rich environment.

Industry Spotlight: Construction

Twenty-two distinct threat actors claimed construction victims in Q1 2026. The top four – Qilin, Play, Akira, and DragonForce – accounted for 72 victims or 55% of all construction victims. Qilin led this category with 26 victims (20%), continuing its multi-quarter dominance in targeting this sector. Play more than doubled its construction presence QoQ from 7 to 16 victims, making up 12% of the total. DragonForce nearly doubled as well, from 8 to 15 (11%). Both growth rates outpaced each group's overall expansion, suggesting the construction industry is a deliberate focus rather than incidental targeting. Akira maintained a consistent 15 victims across both Q4 2025 and Q1 2026 (11%), with targets skewing toward mid-to-large US contractors. Clop tripled its construction count from 4 to 12 (9%), though GRIT notes that Clop's intermittent bulk-posting behavior may inflate single-quarter figures relative to actual intrusion timing.

The construction sector's counter-trend growth in victim counts, combined with independent convergence from multiple threat actors, suggests sustained and increasing targeting activity going forward. With no single group accounting for more than 20% of observed victims and 22 distinct actors active across the quarter, the threat is broadly distributed rather than concentrated, which suggests a structural pattern rather than an artifact of any single group's focus.

GRIT assesses that construction will remain among the five most impacted industry verticals through Q2 2026. Organizations in the sector, particularly specialty contractors and firms with government or enterprise relationships, should treat elevated ransomware exposure as a baseline operating condition. Priority mitigations include remote access hardening, vendor network segmentation, and data loss prevention controls.

Industry Spotlight: Construction Mitigations and Detections

Mitigations:

- **Secure Supply Chain Relationships.**
  Establish cybersecurity requirements for subcontractors, suppliers, and third-party project management platform users. Conduct vendor security assessments before granting system access, monitor third-party connections for anomalous activity, and ensure all parties implement baseline security controls including MFA and endpoint protection.

- **Protect and Segment Sensitive Project Data.**
  Implement network segmentation to isolate project management systems and financial applications. Enforce RBAC that limits users to only the projects and data required for a user's specific role.

- **Secure Field Worker Access.**
  Deploy EDR on field devices, enforce device compliance requirements before granting network access. Use conditional access policies that evaluate device health and location context before allowing connections.

Detections:

- **Detect Email Compromise Targeting Financial Transactions.**
  Monitor for email authentication failures, suspicious invoice modifications, and unauthorized changes to payment receipt details.

- **Alert on Suspicious Activity to Sensitive Project Files.**
  Detect unusual administrative account activity, access to files outside of normal business hours, downloads of entire project directories, and access to financial systems by non-finance users.

- **Detect Supply Chain and Third-Party Access Anomalies.**
  Monitor for unusual VPN connections from subcontractor networks, after-hours access by vendor accounts, privilege changes for third-party users, and data access by partners outside their assigned projects. Track external entity connections to project management platforms and flag behavioral changes like bulk downloads or access attempts to unrelated projects.

Other Reporting and Events

Challenges and Approaches to Data Leak Sites

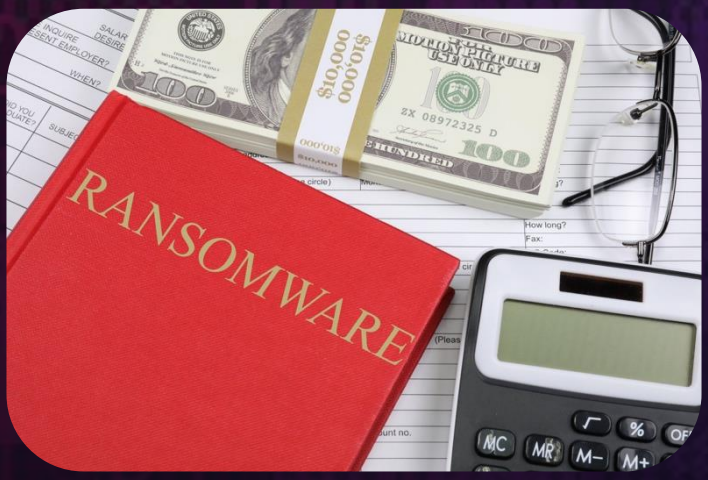
Double extortion has defined ransomware operations for several years, becoming standard ransomware tradecraft after being popularized by Maze in 2019. The tactic combines data exfiltration with traditional ransomware encryption. In addition to deploying ransomware, threat actors also steal data from victim networks and threaten to publish it on the ransomware group's data leak site (DLS) unless the victim pays. This method has been effective because, for many organizations, the perceived legal exposure or reputational risk from a public data leak is greater than the cost of the ransom itself.

Over the past year, GRIT has observed some ransomware groups eschewing the typical encryption stage of ransomware entirely, instead focusing exclusively on data exfiltration as the basis for extortion. That said, operating a DLS is a resource-intensive operation. Publishing stolen data is operationally expensive. GRIT has observed consistent delays between victim compromise and data publication on group DLS infrastructure. This is a reflection of the cost and complexity involved in hosting large datasets anonymously. Some groups have begun leveraging torrents and third-party file-sharing services to reduce that burden. These adaptations are not incidental; they reflect a broader tension between the operational demands of the double extortion model and the infrastructure costs required to sustain it.

To be taken seriously by future targets, ransomware operators must follow through on their threats to post victim data for the victims who do not pay. For obvious reasons, this must be done anonymously as operators prefer not to make their real-life identity easily available to law enforcement. This rules out most commercial file sharing solutions which, in most cases, must abide by know your customer (KYC) regulations and subpoenas on their customer data from law enforcement. Illicit data on legitimate commercial platforms is also short-lived as most have terms and conditions and abuse policies that they must abide by. This has forced many threat actors to create their own infrastructure for file sharing.

Challenges and Approaches to Data Leak Sites

Major ransomware operators now maintain dedicated leak sites hosted as hidden services on Tor to "name and shame" victims. Historically, all groups posted leaks on simple websites run as hidden services on Tor, but that presented practical challenges. By design, Tor prioritizes anonymity over transfer speeds. To maintain anonymity, data is routed through several Tor nodes. Each "hop" through a node increases latency, considerably slowing download speeds. This issue is manageable when hosting static webpages, but latency is a material limitation when distributing large datasets typical of ransomware operations. Hosting costs further compound the problem. Most threat groups use virtual private servers (VPS) disguised by Tor to host their data leak sites, and associated storage costs scale alongside data volume. For smaller or less established groups, these infrastructure costs represent a meaningful operational burden. This means that even nonpaying victims represent a significant cost burden on the responsible threat actor. The data must be stored and hosted regardless of whether the group collects a ransom payment.



Like most infrastructure decisions, the major ransomware players all take different approaches to solving the stolen data hosting problem. Recently Akira has distributed stolen data via torrents. The group generates one torrent per victim and posts the resulting magnet links on their traditional data leak site for mass consumption. The benefit of distributing data this way is that hosting requirements are minimal. GRIT has observed Akira “seeding” these torrents, which often contain upwards of a terabyte of data, using traditional “seedbox” and VPS solutions. Because of the peer-to-peer nature of the torrent protocol, anyone attempting to download these caches of stolen data assist the actor by sharing pieces of the download with their peers. This is not a perfect solution; however. There are a few downsides that have prevented other groups from adopting this approach at scale.

Challenges and Approaches to Data Leak Sites

Sharing files via torrents allows for much less anonymity than most actors would be comfortable with. Every peer connected to a torrent can “see” the IP address and metadata of every other peer. This presents an opportunity to tie both the actor and anyone attempting to download the data to a piece of infrastructure that is theoretically actionable by law enforcement. Steps can be taken to anonymize this connection; however, most would presumably prefer not to take the risk. In addition, sharing this stolen data requires at least one seeder to be present. If the actor is unable to continue seeding a torrent, and no full copies exist for peers to pull from, the underlying data is essentially impossible to download. Akira appears to have operationalized this approach to sharing data, which shows that they are comfortable with the potential downsides. Whether or not they will continue to share data this way in 2026 will likely rely on how well this approach scales.

Throughout their operational life, Qilin has taken a few different approaches towards sharing stolen victim data. For a period of time, the group shared victim data via clear web hosted File Transfer Protocol (FTP) servers whose credentials they shared on their dark web data leak site. This was predictably unreliable for the group as these servers would constantly fall offline, either due to law enforcement action or abuse complaints submitted to their underlying hosting solutions. As the FTP approach proved itself unsustainable, and as the group itself grew considerably by victim volume, the group tried several more solutions. One approach was the use of clear net file sharing solutions like Mega. The actor was able to use this service to host large collections of data and simply provided a download link on their dark web site. This was a convenient approach for the actor, as they did not have to worry about anonymization or hosting issues. The downside is that websites like Mega are at the mercy of requests from law enforcement, and as a result, the shared links to stolen content were often short lived. Now, Qilin seems to have returned to the traditional approach of sharing stolen data via a Tor hosted leak site. This creates a series of ongoing challenges for the group, including significant downtime and large caches of data becoming unavailable. These challenges are accelerated by Qilin’s exponential growth in 2025.

As 2026 continues, GRIT will continue to monitor ransomware groups both small and large for new tactics and approaches towards solving the problem of hosting stolen data at scale. When presented with challenges like this in the past, ransomware gangs have shown willingness to rapidly adopt new techniques. While none of the tactics outlined here are “perfect,” perhaps a group will discover a way to share large caches of stolen data in an anonymous, inexpensive, and highly available way.

Scattered Spider, Lapsu$, Shiny Hunters, Scattered Lapsu$ Hunters: What's the Difference?

In August 2025, three established cybercrime groups – Scattered Spider, LAPSUS$, and ShinyHunters – announced they would merge as "Scattered LAPSUS$ Hunters." While media reporting characterized this as a dangerous new alliance, analysis indicates the development more likely represents a rebranding of overlapping membership and existing operational collaboration, rather than a formal organizational merger. This distinction is critical for defenders: the "merger" publicly formalized what had been true operationally for years. The same individuals conducting operations under the Scattered Spider, ShinyHunters, and LAPSUS$ brands began marketing their activities under a unified name, but the techniques, infrastructure, and targeting remained consistent.

Logos used by Scattered Lapsus$ Hunters, Lapsus$, and ShinyHunters
Source: Ransomlook

The Component Groups and "The Com" Ecosystem

Scattered Spider emerged in May 2022 and quickly established itself through the "0ktapus" campaign (March-July 2022). This campaign is widely documented to have compromised 9,931 accounts across more than 130 organizations through vishing, SMS phishing, SIM swapping, and MFA fatigue attacks. The group operates with exceptional speed compared to traditional ransomware operators. It typically moves from initial access to impact in 24-48 hours rather than weeks or months. Notable operations include the September 2023 alleged attacks against MGM Resorts and Caesars Entertainment. Industry reporting indicates that since 2022, Scattered Spider has infiltrated over 100 businesses and generated over $66 million in documented extortion demands.

Scattered Spider, Lapsu$, Shiny Hunters, Scattered Lapsu$ Hunters: What's the Difference?

ShinyHunters gained prominence in 2025 for large-scale vishing campaigns targeting Salesforce customers. The May 2025 campaign compromised more than 20 organizations across North America and Europe through voice phishing calls that convinced employees to authorize malicious applications disguised as legitimate tools like "Data Loader." The collective claims to have exfiltrated approximately 989.45 million Salesforce records. LAPSUS$ was assessed as largely inactive following member arrests in 2022, making the 2025 return notable. The group differentiated itself through performative publicity by cultivating visibility through Telegram channels and data sample leaks.

Within Scattered LAPSUS$ Hunters, LAPSUS$ is believed to provide the publicity machine and insider recruitment capabilities, actively recruiting employees at telecommunications companies, software corporations, and hosting providers for VPN or Citrix network access rather than data.

All three groups operate within "The Com," a loosely organized English-speaking cybercrime ecosystem of approximately 1,000 individuals according to FBI warnings. The Com operates across distributed Telegram and Discord servers where knowledge, tools, techniques, and opportunities are shared among participants. The ecosystem lacks formal hierarchy or membership requirements. Participation is fluid, with individuals joining operations based on opportunity and capability. Members are predominantly teenagers and individuals in their early twenties, and they are commonly with native U.S. or UK English proficiency. This decentralized structure creates significant attribution challenges, as the same individuals often operate simultaneously under multiple group names.

Scattered Spider, Lapsu$, Shiny Hunters, Scattered Lapsu$ Hunters: What's the Difference?

The "Merger": Rebranding Existing Collaboration

Operational collaboration existed between these groups before the Scattered LAPSUS$ Hunters brand emerged in August 2025. The observed division of labor – with Scattered Spider providing initial access, ShinyHunters handling data exfiltration and cloud exploitation, and LAPSUS$ providing publicity and extortion pressure – predated the unified branding. Attack TTPs in Scattered LAPSUS$ Hunters-attributed operations reflect those of the individual groups:

- The May 2025 Salesforce vishing campaign matches ShinyHunters methodology
- Insider recruitment echoes LAPSUS$ tactics
- Rapid exploitation reflects Scattered Spider operational tempo

Rather than reflecting actual changes in capabilities or membership, the strategic rationale for rebranding centers on marketing advantages. Combining three established brands multiplies perceived threat level. Victims receiving Scattered LAPSUS$ Hunters extortion demands face the perceived combined capabilities of all three groups. The "merger" narrative generated significant media attention, serving multiple purposes: victim intimidation, recruitment within The Com, and credibility in underground forums. Organizations may perceive elevated risk from a "merged" threat actor, potentially influencing ransom payment decisions.

In November 2025, the group released ShinySp1d3r ransomware-as-a-service, reinforcing the marketing focus. The name explicitly combines "Shiny" from ShinyHunters and "Sp1d3r" from Scattered Spider. The RaaS model allows affiliates to access the Scattered LAPSUS$ Hunters brand and infrastructure through profit-sharing arrangements.

Scattered Spider, Lapsu$, Shiny Hunters, Scattered Lapsu$ Hunters: What's the Difference?

"Rey" and Attribution Fluidity

The identification of "Rey" illustrates why traditional group attribution provides limited value in The Com ecosystem. In November 2025, Rey was identified as an administrator of the Scattered LAPSUS$ Hunters Telegram channel and technical operator behind ShinySp1d3r ransomware. Investigation traced Rey's identity to Saif Al-Din Khader, 15 years old, based in Amman, Jordan. Rey participated in multiple groups simultaneously as the Hunters Telegram administrator, Hellcat ransomware data leak site administrator, BreachForums administrator, and member of Cyb3r Drag0nz Team, a pro-Palestinian hacktivist group. Rey described ShinySp1d3r as "just a rehash of Hellcat ransomware, except modified with AI tools" (Krebs, 2025). This demonstrates how ransomware code flows between operations with different branding applied to similar underlying tools.

Despite significant operational security failures that led to his identification, this 15-year-old served as technical operator for globally impactful cybercrime operations. This case illustrates that individuals participate in multiple "groups" simultaneously without exclusive membership in any single organization. The same person's activities span what appear to be distinct threat actors but represent a single individual operating under different identities across The Com ecosystem.

Former display page of "Hellcat" ransomware
Source: Ransomlook

Scattered Spider, Lapsu$, Shiny Hunters, Scattered Lapsu$ Hunters: What's the Difference?

Retirement Announcement and Implications for Defense
Between August and October 2025, Scattered LAPSUS$ Hunters announced retirement from cybercrime operations. This announcement warrants skepticism given historical patterns of false retirements. ALPHV/BlackCat, DarkSide, REvil, and Conti all announced retirements before rebranding or resuming operations, typically to reduce law enforcement scrutiny. LAPSUS$ itself was assessed inactive after the 2022 arrests, yet reemerged in 2025, further limiting the credibility of retirement claims from these actors.

Additionally, the nature of Scattered LAPSUS$ Hunters decentralized structure prevents enforcement of retirement decisions. Even if current administrators cease activity, hundreds of ecosystem participants can continue using techniques, tools, and branding without coordination. ShinySp1d3r ransomware exists, social engineering methodologies are documented, and victim shaming infrastructure is built. That means that financial incentives to continue operations exist regardless of group names.

Organizations should treat retirement announcements from decentralized cybercrime collectives as operationally meaningless and maintain defensive measures against documented TTPs regardless of group status. Resources spent tracking group names or analyzing merger implications are resources not allocated to defensive fundamentals. Group-centric attribution can become misleading when:

- Individuals simultaneously participate in multiple "groups"
- Retirements are announced but techniques persist
- "Mergers" represent branding decisions rather than organizational changes

Understanding that reality, organizations can then focus defensive resources on TTPs rather than threat actor attribution by implementing:

- Rigorous caller verification for help desk operations
- Phishing-resistant MFA
- Administrative approval requirements for third-party app integrations
- Anomaly detection for data access and exfiltration

These additional controls addressing social engineering, credential theft, and unauthorized application access remain effective regardless of what threat actors call themselves, protecting organizations from these groups' tactics.

Scattered Spider, Lapsu$, Shiny Hunters, Scattered Lapsu$ Hunters: What's the Difference?

Mitigations and Detections

Mitigations

- **Strengthen Social Engineering Defenses.**
  Educate all employees on adversary social engineering tactics, including MFA fatigue attacks, impersonation calls, and recruitment attempts. Establish clear reporting channels for suspicious contacts and create a security-conscious culture where employees verify unusual requests through separate communication channels.

- **Implement Phishing-Resistant MFA.**
  Deploy FIDO tokens or biometric authentication like Windows Hello instead of SMS or simple push notifications. Organizations should also establish strict policies against sharing MFA between users.

- **Protect Against Credential Theft.**
  Deploy password protection to prevent weak passwords, implement password managers, and actively scan code repositories and collaboration platforms for exposed credentials.

Detections

- **Alert on Anomalous Authentication Patterns.**
  Alert on geographic anomalies and user accounts authenticating from multiple locations within a short timeframe. Leverage tools to identify risk sign-ins and credential replay attacks using stolen session tokens that bypass standard MFA.

- **Identify Data Exfiltration and Reconnaissance.**
  Monitor for bulk searches of data in SharePoint sites and large data transfers to personal storage or unknown infrastructure. Track creation of virtual machines in cloud environments and establishment of unauthorized transport rules in email systems that forward communications to attacker-controlled accounts.

- **Monitor Cloud Tenant Changes.**
  Alert on high-risk modifications including changes to Azure AD roles, creation or modification of Exchange transport rules, and unusual API token generation. Investigate unauthorized device enrollments, MFA method changes, and any impersonation session events in identity platforms that could indicate persistence.

Open Claw and Malicious Skills

In February 2026, VirusTotal reported the first confirmed, large-scale supply chain attack against an agentic AI platform, targeting OpenClaw's skills marketplace. A threat actor published over 314 malicious skills that delivered information-stealing malware disguised as legitimate automation tools. In this attack, actors exploited a structural characteristic of AI agent platforms: skills are instruction-based rather than code-based. This allowed attackers to evade traditional malware detection. Users were directed to download and execute external payloads disguised as “setup procedures," resulting in credential theft, persistent backdoor access, and system compromise. This incident marks a notable shift where agentic AI systems have transitioned from theoretical risks to operational targets.

Source: GitHub

The campaign targeted “skills” within agentic AI platforms. Traditional AI chatbots can only provide answers to prompts based on the knowledgebases they have been trained on. Agentic AI can autonomously decompose complex objectives into multi-step execution plans, interact with systems using tools and APIs, and pursue goals without continuous human oversight. This is in contrast to traditional AI “chat bots,” which can simply provide answers to prompts.

OpenClaw is an open-source agentic AI that runs locally with direct access to shell commands, file operations, and network requests. Users can extend its capabilities by downloading additional skills from the ClawHub marketplace. Here, the malicious skills were presented as benign utilities, such as "Yahoo Finance" or "Crypto Analytics." The skills contained setup instructions directing users to download either password-protected executables or Base64-encoded shell scripts, depending on the users’ operating systems. After users followed the skill’s instructions, the information stealing payloads were then delivered.

Open Claw and Malicious Skills

The delivery mechanism for the malware bypassed traditional security controls because the malicious behavior was emergent rather than hardcoded. The skill files themselves contained no malware and produced no antivirus detections. Instead, the threat laid in the workflow. Infections resulted from trusted instructions executed by a trusted AI agent, with the human user acting as the interpreter translating benign text into malicious action. Organizations must recognize that AI agents are a trust boundary where supply chain security, behavioral monitoring, and least-privilege access controls are critical.

OpenClaw responded by partnering with VirusTotal to deploy automated security scanning across all ClawHub skills. Scans include SHA-256 hash lookups against VirusTotal's threat database and uses Gemini-powered Code Insight to analyze skill packages for suspicious patterns including remote code execution instructions, external file downloads, obfuscated scripts, and unsafe command execution. Now, skills receive automated verdicts and are re-scanned daily to detect new threats. OpenClaw recognizes this system is imperfect, however, since prompt injection payloads and novel attack techniques may evade detection. Although not comprehensive, OpenClaw is free to determine its own security prerogative. The AI agent ecosystem currently lacks industry-standard threat models, specialized detection tools, and security-focused regulatory guidance.

This campaign demonstrated that agentic AI adoption without a security-first architecture creates unacceptable risk. With at least 314 malicious skills delivering real malware, it proves this threat is operational, not theoretical. As agentic AI platforms gain enterprise adoption, security teams should require granular access controls, mandatory extension scanning, audit logging, and incident response capabilities.

Open Claw and Malicious Skills Mitigations and Detections

Mitigations

- **Harden Gateway Exposure and Authentication.**
  Implement Zero Trust Network Access (ZTNA) controls that require device compliance verification before allowing API access. Deploy API gateways with rate limiting, IP allowlisting, and WAF rules to prevent unauthorized automation attempts.

- **Patch Internet-facing Systems and Dependencies.**
  Regularly update OpenClaw to the latest stable version (`openclaw update –channel stable`) and run `openclaw doctor` after each update to identify security misconfigurations or depreciated settings. Monitor the OpenClaw security advisories and apply patches for any disclosed vulnerabilities.

Detections

- **Detect Suspicious Tool Invocation Patterns.**
  Monitor for rapid-fire AI calls across multiple tools, unusual tool chaining sequences that deviate from established workflows, and high-volume data extraction through read/search operations.

- **Identify Message Injection and Prompt Manipulation.**
  Analyze incoming messages across all channels for indicators of prompt injection attacks, including messages with excessive system-role instructions, attempts to override safety guardrails (“ignore previous instructions”), or encoding tricks (base64, Unicode substitution, markdown abuse) designed to bypass input validation.

- **Track Anomalous Gateway Network Activity.**
  Monitor for unusual connection patterns including traffic spikes from a single IP address, connections from anonymizing services or unexpected geographic locations, and off-hours API access that deviates from normal business patterns.

- **Audit Channel Configuration Drift.**
  Implement configuration monitoring to detect unauthorized changes to OpenClaw’s `openclaw.json` file. Use file integrity tools or version control for configuration files, and trigger alerts when high-risk settings are modified.

Q1 2026 Iran Cyber Update

In our Q2 2025 report, we assessed that Iranian cyber operations following the June 22 nuclear facility strikes would remain regionally targeted and measured, with Iranian leadership appearing to recognize the limitations of cyber retaliation against adversaries' superior kinetic capabilities. Eight months later, that assessment has largely held, but the operational landscape has evolved in ways that warrant attention.

What has emerged is a blend of state-sponsored cyber operations under hacktivist cover, characterized by:

- Opportunistic data destruction
- Influence operations that exceed actual impact
- The weaponization of historical breaches for current psychological warfare

Iranian Ministry of Intelligence and Security (MOIS) fronts, including the Handala Hack Team, have shifted from espionage-focused operations to tactically disruptive attacks designed to impose economic costs and signal resolve while maintaining plausible deniability.

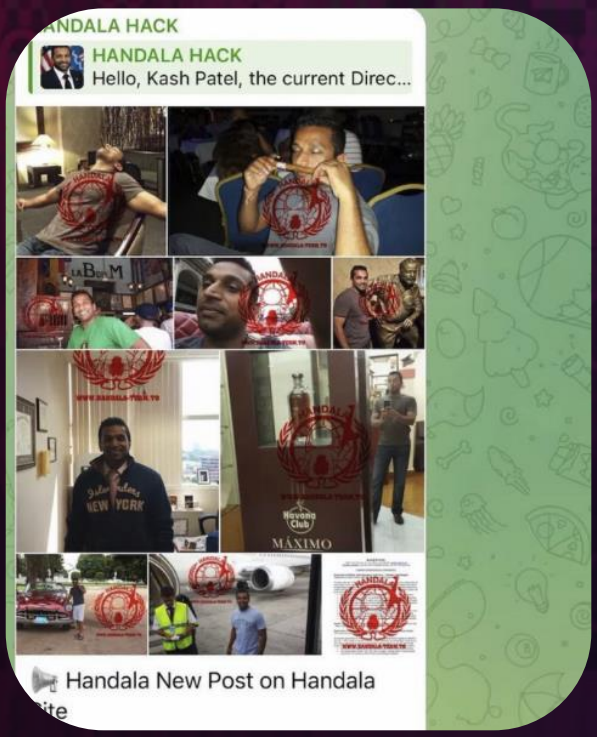
Hacktivism

The Handala Hack Team has emerged as a prominent hacktivist persona with suspected ties to Iran's MOIS. Security researchers have traced what may be Handala's origins to earlier operations conducted under different names, including Homeland Justice, which deployed destructive wiper malware against Albanian government agencies in 2022. Following the February 28, 2026, U.S. and Israeli strikes on Iran, Handala operations shifted from primarily regional targeting to include U.S. homeland attacks characterized by data destruction rather than traditional espionage.

Q1 2026 Iran Cyber Update

On March 11, 2026, Handala claimed responsibility for a destructive malware attack against Michigan-based medical technology firm Stryker, reportedly disabling tens of thousands of systems and paralyzing global operations. The group framed the attack as retaliation for the Minab school strike that killed more than 160 civilians. Security researchers characterize Handala as having "combined the noisy, chaotic playbook of a hacktivist group with the destructive capabilities of a nation-state."

The operational sophistication demonstrated in the Stryker breach represents a shift from intelligence collection to disruptive impact. The group has deployed data-destroying wiper malware variants including Coolwipe, Chillwipe, and Bibiwiper. These tools prioritize destruction over persistence, suggesting operational objectives focused on immediate disruption rather than sustained access for intelligence gathering. Wiper attacks represent the worst-case scenario for victim organizations: unlike ransomware, there is no payment option for recovery, only restoration from backups if they exist and remain accessible.



Part of Handala's claims to have breached the emails of FBI Director, Kash Patel
Source: Telegram

Then, on March 27, 2026, Handala claimed responsibility for breaching FBI Director Kash Patel's personal email account, posting historical personal photos and documents. The FBI confirmed awareness of "malicious actors" targeting Patel's email information but indicated the compromised material was "historical in nature" and contained "no government information." Security researchers assessed the breach likely represented recycled data from an earlier 2024-2025 compromise rather than a sophisticated new operation. This illustrates a pattern in Iranian-aligned hacktivist operations: the weaponization of historical breaches for current psychological operations.

Q1 2026 Iran Cyber Update

The U.S. Justice Department's March 19, 2026, action seized four domains (Justicehomeland[.]org, HandalaHack[.]to, Karmabelow80[.]org, and HandalaRedwanted[.]to) that the DOJ characterized as facilitating suspected MOIS "hacking efforts tied to psychological operations and transnational repression." Court documents supporting the seizure warrant detailed how the infrastructure operators used these domains to post stolen personally identifiable information, claim credit for hacking operations, and issue death threats to Iranian dissidents, journalists, and Israeli persons. The affidavit documented emails offering bounties to Mexican cartel "partners" for violence against Iranian dissidents in the United States and abroad.

Handala operations demonstrate a hybrid model combining technical intrusion capabilities with psychological operations designed to maximize political impact. However, hacktivist groups – such as these Iran-aligned groups in particular – are known for lying, obfuscating, and exaggerating their impact. In some cases, "recent" attacks are not recent at all, but they are being weaponized for publicity and sensationalism. Post-hoc justifications for targeting appear opportunistic: in Stryker's case, the rationale included a 2019 acquisition of an Israeli company. In other attacks, "they are a U.S. company" has been sufficient justification.

Security researchers assess that Handala operations "don't have the hallmarks of a plan", but rather represent efforts to identify and exploit targets of opportunity to demonstrate retaliatory capability. This assessment suggests tactical sophistication without strategic coherence — what one researcher characterized as "thrashing for targets."

Influence Operations and Kinetic Threats Blend

On April 1, 2026, Iranian state media and the Islamic Revolutionary Guard Corps (IRGC) issued statements threatening 18 major technology companies operating in the Middle East, including U.S.-based Microsoft, Google, Apple, Meta, Oracle, Intel, HP, IBM, Cisco, Dell, Palantir, Nvidia, Tesla, JP Morgan, GE, and Boeing, as well as UAE-based G42 and Spire Solutions. "These companies should expect the destruction of their respective units in exchange for each terror act in Iran, starting from 8pm Tehran time on Wednesday, April 1st," the IRGC statement warned, calling the companies "key institutions involved in terrorist espionage operations."

Q1 2026 Iran Cyber Update

The threatened deadline passed without widespread reported incidents, though Amazon Web Services facilities in Bahrain were struck the following day, causing fire damage to cloud computing infrastructure. AWS facilities in the region have been struck multiple times during the conflict, suggesting that physical infrastructure investments by U.S. technology companies in the Middle East present attractive targets for imposing economic costs.

Iranian-aligned actors have also released multiple Lego-themed propaganda videos on social media
Source: Fox11 Los Angeles

This blending of cyber threats with kinetic military action represents the operational environment Iranian-aligned hacktivist fronts now operate within. The goal of the Iranian regime throughout appears to have been imposing economic costs on adversaries. Substantial infrastructure investments by major technology companies in the region – data centers, manufacturing facilities, regional headquarters – present more desirable targets than office buildings alone. However, the cyber threat component remains characterized by opportunistic targeting and influence operations designed to amplify psychological impact beyond actual technical capabilities.

Threat Landscape Assessment

Most cyber operations from Iranian-aligned actors function as half influence operation and half real impact. Threatened "destruction" may manifest as small hack-and-leak operations or website defacement rather than comprehensive infrastructure compromise. The Stryker breach, while genuinely disruptive to the company, did not represent strategic infrastructure targeting. The Patel email compromise involved historical personal data rather than classified government information. The 120+ Iran-affiliated hacktivist groups maintain DDoS campaigns and hack-and-leak operations focused on symbolic rather than strategically significant targets.

The feared scenario of sustained homeland-targeted destructive campaigns against critical infrastructure has not yet materialized. What has emerged: tactically opportunistic operations targeting accessible vulnerabilities for immediate disruptive effect, amplified by influence operations that exaggerate impact and capabilities.

Q1 2026 Iran Cyber Update

Forward-Looking Considerations

Several threat vectors warrant monitoring based on observed behavior patterns:

Data Destruction: The shift to destructive wiper malware represents a tactical evolution prioritizing immediate disruption over sustained intelligence collection. Defense follows the same principles as ransomware — defense in depth, strong identity controls, immutable backups — but with higher stakes since there is no payment option for recovery. Organizations should verify backup integrity and restoration procedures for business-critical systems.

Influence Operations: Organizations should develop protocols to rapidly assess breach claim veracity for technical response and stakeholder communications. False or exaggerated claims serve psychological warfare objectives, and the weaponization of historical breaches as current attacks complicates threat assessment and response prioritization.

Opportunistic Targeting: Target selection appears driven by accessibility rather than strategic value. Organizations with internet-facing infrastructure containing unpatched vulnerabilities or weak credentials represent primary exposure vectors. Post-hoc justifications include tenuous connections like historical acquisitions of Israeli companies or simply being a U.S. entity. The threat landscape suggests broad scanning for vulnerable targets rather than sophisticated long-term campaigns.

Regional Physical Infrastructure: Organizations with substantial Middle East investments (data centers, manufacturing facilities, regional headquarters) should evaluate kinetic targeting exposure. The pattern of attacks against AWS facilities suggests horizontal targets of opportunity.

Personal Account Targeting: Personal email accounts lacking enterprise-grade protections remain attractive targets for embarrassing or collecting intelligence on individuals in positions of authority. Organizations may consider guidance for executives and high-risk personnel, particularly those with public profiles or regional ties.

Organizations not directly involved in the regional conflict or operating in the Middle East may evaluate whether the current threat landscape warrants threat-specific countermeasures beyond baseline security hygiene. Organizations may assess their specific risk exposure based on operational footprint, regional involvement, supply chain dependencies, and profile visibility when determining appropriate defensive postures.

CISA's June 30th, 2025, advisory confirmed no specific credible threats from Iran currently target U.S. critical infrastructure, though the agency continues encouraging review of threat bulletins as conditions evolve. This assessment should be treated as current but subject to change.

Quarterly Wrap Up

Quantitatively, the first quarter of 2026 can be viewed as “business as usual” in the ransomware ecosystem. Other than some ebbs and flows in activity among distinct ransomware groups, we observed neither substantial increases nor decreases in operational activity QoQ or YoY. This can be explained by both a relative lack of new significant disruptive players in the space, as well as potential increasing market saturation leading to reduced “spread” of actors over time. However, after several years of tracking the ransomware economy, we have unfortunately learned that periods of relative normalcy have often been short lived. While it is impossible to predict what the rest of the year will bring, history suggests we will likely see the arrival or departure of at least one major threat group – whether by internal infighting, law enforcement disruption, or pressure from other groups.

One trend to watch as we enter the middle of the year is the "summer slowdown" in victim claims that nearly always occurs between Q2 and the beginning of Q3. In previous years, even after a frenzied start, we have observed a decrease in victim posts that we have assessed (only slightly tongue-in-cheek) to be the result of summer vacations or mid-year hiatus by threat actors seeking to enjoy the warm weather and take a break from screen time. If 2026 continues this trend, expect to see slightly lower numbers in Q2.

For all the relative “good news” of a quarter not exponentially increasing, we have new concerns and topics to focus on. Iran’s deputized, aligned, or state-sponsored threat groups, including nominal “hacktivist” groups, such as Handala, pose largely unsophisticated but real threats to U.S. and Western organizations while tensions and kinetic operations persist in the Middle East. In many cases, successful operations by these groups are more notable for their psychological effects than their disruptive impacts in real terms, but significantly destructive outlier cases have occurred and cannot be ignored. Fortunately, the preventive measures that have been prescribed in recent years for ransomware and general cybercrime are similarly effective against many of these types of actors, so there is no need to “reinvent the wheel.” Application of security best practices, hardening of the perimeter, and validation of controls and processes remain high-ROI steps that Defenders can take.

In this quarter’s report, we tried to take a little extra time to focus on detection and mitigation opportunities to accompany our reporting – we hope that you will consider these and other recommendations throughout the report in making your environments that much more secure, resilient, and prepared through the rest of 2026.

Happy Hunting!