BRANDEFENSE

RANSOMWARE TRENDS REPORT Q1/2026

COMPARISON WITH Q4 / 2025

Contents

PART I

Executive Summary

High-level assessment of the global ransomware threat landscape, headline statistics, and the critical findings that define the current reporting period ending April 07, 2026.

2286	Total victim posts monitored
2135	Confirmed ransomware incidents
93.4%	Post confirmation rate
68	Distinct threat actor groups
Qilin	Highest-volume operator
Manufacturing	Most targeted sector
United States	Most targeted country

Executive Summary

2286	2135	151	68
TOTAL VICTIM POSTS	CONFIRMED VICTIMS	PENDING REVIEW	ACTIVE GROUPS

The Brandefense Cyber Threat Intelligence (CTI) team monitored **2286** ransomware victim posts spanning **68** distinct threat actor groups during the period ending **April 07, 2026**. Of these, **2135** cases (**93.4%**) have been independently verified as confirmed incidents, while **151** posts remain under analysis. The elevated confirmation rate reflects operational maturity: modern operators publish proof-of-exfiltration data samples alongside victim listings to establish credibility, reducing the proportion of unverifiable claims relative to earlier periods in the ecosystem's development. This evidentiary discipline also signals that operators increasingly understand the negotiation leverage that credible data disclosure threats provide, investing accordingly in pre-encryption exfiltration as a standard operational step rather than an optional pressure tactic.

Qilin leads all tracked groups with **363** attributed victims (**15.9%** of group-attributed activity), followed by **TheGentlemen** (183) and **Akira** (177). The top three operators collectively hold **31.6%** of victim share; the top ten account for **65.9%**. This concentration profile is a hallmark of a mature Ransomware-as-a-Service ecosystem in which platform operators achieve dominant market positions by offering affiliates superior tooling quality, reliable payment infrastructure, and revenue-sharing rates that create strong switching costs. The remaining 58 operators — while individually lower-volume — collectively represent a structurally important and dynamic portion of the landscape, encompassing both growing mid-tier programs and newly launched entrants fuelled by commoditised builder toolkits.

The **Manufacturing** sector holds first position among targeted industries with **397** victim organisations — a position driven by OT/IT convergence, production-line downtime pressure, and high ransom payment capacity. Geographically, **United States** accounts for **1084** victims (**49.4%** of country-specific targets). Western nations collectively represent **24.0%** of specifically identified victims — likely an underestimate due to differential reporting frameworks across regions.

► **Methodology — Data Curation Transparency:** 2286 total victim posts were collected for the monitoring period. Of these, **2135** (93.4%) are confirmed ransomware incidents. **151** are PENDING active analysis, with the remainder classified as DUPLICATE or REJECTED (misidentified victims, operator error, or confirmed fabrications). The 2135 confirmed figure is the basis for all statistical analysis in this report. Filtering methodology: posts are cross-referenced against public breach confirmations, partial data samples, and third-party IR disclosures before status assignment.

Key Findings & Severity Assessment

Dominant Operator: Qilin — 363 victims, 15.9% of tracked activity. Multi-platform encryptor with dedicated VMware ESXi payload sustaining operational tempo across all primary target sectors.

Market Concentration: Top 3 groups: 31.6% of activity. Top 10: 65.9%. The remaining 58 operators account for 34.1% — significant in aggregate and indicative of a broad, resilient affiliate ecosystem.

Primary Sector Risk: Manufacturing (397), Technology (364), Business Services (219). The top three sectors represent 45.9% of industry-identified victims. Healthcare's structural payment dynamics will sustain its top-ranked position absent sector-wide defensive investment.

Geographic Concentration: United States — 1084 victims (49.4%). Western nations: 24.0% of country-specific targets. Remaining 87 countries account for additional victims reflecting both genuine global spread and emerging market targeting diversification.

Activity Peak & Trajectory: March 2026 — 824 posts (period high). Most recent period increased by 55 posts (7%) month-over-month. Trajectory: **upward**. Insufficient historical data for quarter-over-quarter comparison.

ESXi Targeting Maturity: 11 major operators deploy dedicated hypervisor encryptors. ESXi-level ransomware is now a baseline RaaS capability — organisations without hypervisor-specific backup isolation face compounded incident severity.

Quarter-over-Quarter Analysis: Q4 2025 vs Q1 2026

Data Coverage Note: Q1 2026 covers the full January–March 2026 quarter (complete monitoring window at time of publication). Q4 2025 covers October–December 2025. Both quarters reflect complete monitoring periods — the +50.1% increase in confirmed victim count represents a genuine escalation in ransomware activity, not a data completeness artefact.

METRIC	Q4 2025	Q1 2026	Δ CHANGE
OVERVIEW			
Confirmed Victims	1,422	2,135	▲ +713 (+50.1%)
Active Groups	51	68	▲ +17
Monthly Avg. Victims	474	712	▲ +50.2%
THREAT ACTOR RANKINGS			
Rank 1 Group	Qilin (481)	Qilin (363)	— retained
Rank 2 Group	ClOp (402)	TheGentlemen (183)	▲ new entry
Rank 3 Group	Akira (222)	Akira (177)	— retained
Rank 4 Group	—	IncRansom (141)	▲ new entry
Rank 5 Group	—	ClOp (127)	▼ dropped from #2
SECTOR TARGETING			
Primary Target Sector	Manufacturing (24.1%)	Manufacturing (18.6%)	— retained
Secondary Target Sector	Technology (16.7%)	Technology (17.0%)	—
GEOGRAPHIC REACH			
Top Country	United States (48.4%)	United States (49.4%)	— retained

METRIC	Q4 2025	Q1 2026	Δ CHANGE
Countries Targeted	134 (2025 annual total)	97	—

QoQ Key Observations

1. Qilin dominance persists — but volume softens. Qilin retained the #1 position in both Q4 2025 (481 victims) and Q1 2026 (363 victims), underscoring its structural RaaS ecosystem leadership. The 24.5% decline in attributed victims may reflect affiliate diversification to competing platforms rather than a true operational decline — overall ecosystem volume increased 50.1% in the same period.

2. TheGentlemen: fastest-rising new entrant. TheGentlemen debuted directly at Rank 2 with 183 victims in Q1 2026, making it the most impactful new entrant of the reporting cycle. Rapid ascent from no documented Q4 2025 activity to top-tier status within a single quarter is consistent with an experienced affiliate team migrating from a disrupted platform rather than a genuinely new operator.

3. Akira holds Rank 3 — structural mid-tier stability. Akira maintained third position in both Q4 2025 (222 victims) and Q1 2026 (177 victims). Consistent Cisco VPN exploitation and BYOVD EDR-blinding techniques continue to deliver reliable victim access, indicating a mature, well-resourced affiliate network not subject to the volatility seen in newer entrants.

4. Manufacturing retains top target sector. Manufacturing remained the #1 targeted sector in Q1 2026 with 397 victims, consistent with its Q4 2025 position (24.1%). The sector's structural vulnerability profile — OT/IT convergence, production-line downtime pressure, and high ransom payment capacity — continues to make it the structurally preferred target across all major RaaS platforms.

5. ClOp's sharp decline: from #2 to #5. ClOp dropped from #2 in Q4 2025 (402 victims) to #5 in Q1 2026 (127 victims) — consistent with its campaign-burst operational model. The Q4 2025 surge was driven by the Cleo MFT exploitation campaign; Q1 2026 contraction reflects post-campaign dormancy. A resurgence targeting a new zero-day vulnerability class (MFT platforms, enterprise appliances) should be anticipated within 1–2 reporting periods.

Q2 2026 Intelligence Outlook

Based on Q1 2026 data trends and observed threat actor behaviour patterns, the following Q2 2026 projections apply:

Volume Escalation Continues

HIGH CONFIDENCE

Q1 2026 monthly data shows a clear upward trajectory: January (693) → February (769) → March (824). Q2 2026 is expected to sustain or exceed this pace as affiliates complete campaigns initiated during Q1 recruitment cycles. Brandefense projects Q2 2026 confirmed victim count to exceed 2,200.

TheGentlemen Consolidation

MEDIUM CONFIDENCE

TheGentlemen's direct #2 entry suggests a stabilising affiliate network. If the group maintains its Q1 pace, it is likely to challenge Qilin for the top position within 1–2 reporting periods. Sustained presence at 150+ victims per month would confirm transition from emerging to established RaaS platform status.

ClOp Zero-Day Resurgence

MEDIUM CONFIDENCE

ClOp's campaign-burst pattern (GoAnywhere Q1 2023, MOVEit Q2 2023, Cleo Q4 2025) suggests Q2–Q3 2026 as the likely window for its next mass-exploitation campaign. MFT platforms, enterprise file sharing appliances, and edge network devices with recently disclosed but unpatched CVEs should be treated as highest-priority pre-emptive remediation targets.

Manufacturing & Technology Sectors Remain Primary Targets

HIGH CONFIDENCE

Manufacturing maintained #1 position for consecutive quarters. Technology and Professional Services are trending upward based on Q1 sector data. Organisations in these sectors should anticipate sustained attacker attention and elevated targeting pressure through Q2 2026, particularly from Akira (VPN exploitation) and IncRansom (enterprise application vectors).

PART II

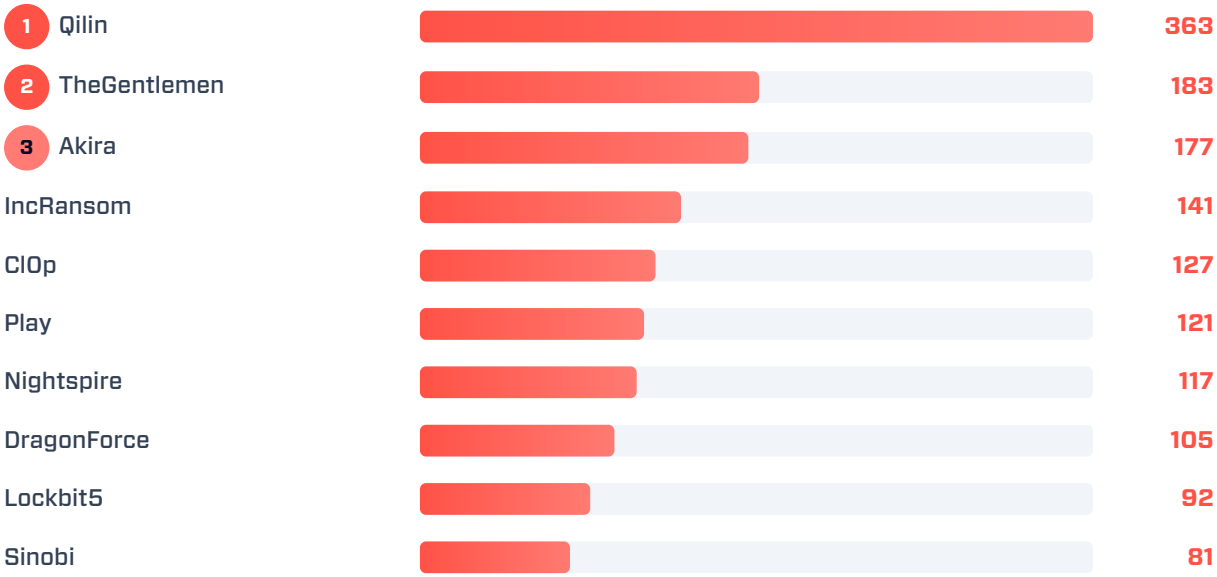
Threat Actor Landscape

Ranking and market analysis of 68 monitored ransomware operators — top 10 by victim count, others summary, and RaaS ecosystem concentration analysis.

363	Qilin
183	TheGentlemen
177	Akira
141	IncRansom
127	ClOp
121	Play
117	Nightspire
105	DragonForce

Top 10 Ransomware Groups by Activity

The ten highest-volume operators are ranked below by total attributed victim count. Bar lengths are normalised relative to **Qilin** (363 victims = 100%). Together, these ten groups account for **65.9%** of all group-attributed victims. The gap between #1 **Qilin** and #2 **TheGentlemen** stands at 180 victims — a 98% margin — signalling structural dominance, not merely first-place ranking. This gap reflects Qilin's superior affiliate attraction capacity through tooling quality and revenue-sharing competitiveness.



Remaining Operator Ecosystem — Others Summary

OTHERS RANK 11–68	**58 additional operators** account for a combined **779 victims** (34.1% of total group-attributed activity). Breakdown by operational tier: 16 High-tier (20–49 victims) · 23 Active (5–19 victims) · 19 Emerging (<5 victims)

Operator Concentration & RaaS Market Analysis

The full operator pool of **68** groups stratifies into three distinct operational tiers. **11 major operators** (50+ victims) represent established RaaS platforms with mature affiliate networks, dedicated negotiation infrastructure, and multi-platform encryptor development. **27 mid-tier operators** (10–49 victims) include growing programs and experienced independent affiliates. The **58** operators beyond the top 10 — covering 16 high-tier, 23 active, and 19 emerging programs — collectively contribute **779 victims**, a volume that would itself rank as a significant independent threat category if treated as a single group.

The **31.6%** combined share of the top three operators in a field of 68 is consistent with a moderately concentrated market undergoing consolidation. Dominant operators create self-reinforcing competitive advantages: affiliates gravitate toward platforms with the highest victim payment probability and most reliable decryption delivery, which further increases the platform's revenue and investment capacity for tooling improvements — creating a cycle that compounds competitive position over time. The 19 emerging operators in the dataset represent the most dynamic and least predictable segment: several are in pre-growth phases that historically precede rapid expansion within 2–4 reporting cycles.

The proliferation of leaked ransomware builders — principally the LockBit 3.0 source code (released September 2022) and subsequent Chaos/Babuk-derived toolkits — is the primary structural driver sustaining the high count of low-volume operators. New entrants can deploy functionally capable ransomware without original development investment, reducing the barrier to program launch to primarily operational and recruitment challenges. This commoditisation dynamic means the total operator count is unlikely to decline materially without either coordinated toolchain takedown or sustained affiliate disruption — neither of which has proven durable against the resilience of decentralised criminal ecosystems.

PART III

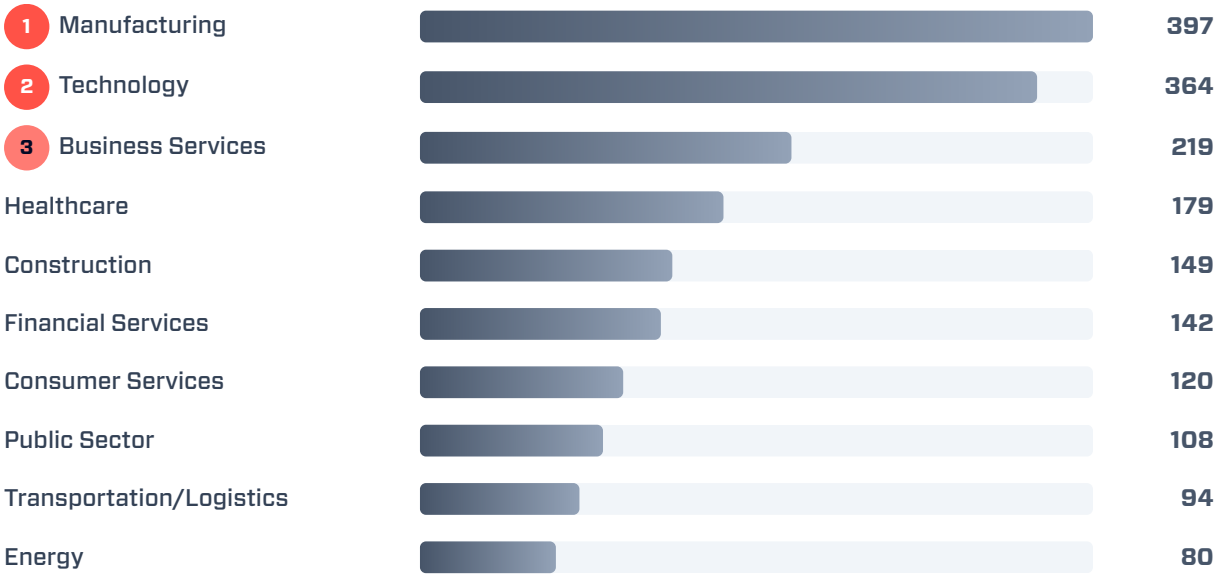
Sector Targeting

Industry-level victim analysis across 16 identified categories — top 10 ranked sectors, others summary, and the economic targeting logic driving affiliate sector selection.

397	Manufacturing
364	Technology
219	Business Services
179	Healthcare
149	Construction
142	Financial Services
120	Consumer Services
108	Public Sector

Top 10 Most Targeted Sectors

Ransomware affiliates are economically rational actors who prioritise sectors with the highest expected payment probability, richest secondary data monetisation potential, and lowest operational access resistance. The top three sectors — **Manufacturing**, **Technology**, and **Business Services** — account for **45.9%** of all industry-identified victims. Bars are normalised relative to the highest-volume sector (Manufacturing, 397 = 100%).



Remaining Sector Coverage — Others Summary

OTHERS RANK 11–16	**6 additional sectors** recorded a combined **283 victims** (13.3% of industry-identified activity). These sectors span energy, telecommunications, government, transport, agriculture, and civil society — reflecting the broad attack surface accessible via commodity initial access vectors independent of deliberate sector selection.

Sector Targeting Commentary & Attack Logic

The **Manufacturing** sector's sustained first-place position reflects a uniquely coercive extortion dynamic. Healthcare organisations operate under patient safety obligations that prevent extended system unavailability, creating ransom decision timelines measured in hours rather than days. Clinical operations depend on real-time access to imaging systems, laboratory platforms, patient record infrastructure, and medical device networks — all simultaneously disrupted by a successful ransomware deployment. Combined with mandatory breach notification obligations under HIPAA, GDPR, and equivalent frameworks that add regulatory penalty exposure to the operational disruption pressure, healthcare organisations face a multi-dimensional coercion environment that consistently produces above-average ransom payment rates, creating a self-reinforcing targeting dynamic.

The co-equal prominence of **Technology**, **Business Services**, and **Healthcare** sectors reflects complementary targeting logic across different value extraction profiles. Manufacturing organisations face production line disruption costs that translate immediately into quantifiable revenue loss, creating strong financial pressure to restore operations without extended delay. Consulting and professional services firms hold privileged client data repositories that enable secondary extortion leverage not only against the firm itself but against its entire client portfolio — a force multiplier for ransom pressure. Technology organisations carry source code, customer credential databases, and cloud infrastructure access tokens that support both direct monetisation and downstream supply-chain targeting opportunities.

The **6** sectors beyond the top 10 — collectively responsible for **283 victims** — demonstrate that ransomware affiliate targeting is not exclusively deliberate sector selection. A significant portion of lower-ranked sector victims result from opportunistic initial access: affiliates purchasing VPN credentials or exploiting internet-facing vulnerabilities at scale, then selecting high-value targets for payload deployment regardless of sector. This opportunistic layer means no sector can

assume low aggregate victim count equates to low individual organisation risk. Defensive posture — MFA coverage, patch currency, backup isolation — is a stronger predictor of incident probability than sector membership.

Sector Macro-Category Analysis

The following table groups all 2135 industry-identified victims into four strategic macro-categories to surface cross-sector attack surface patterns and support risk-tiered defensive investment decisions.

MACRO-CATEGORY	CONSTITUENT SECTORS (SAMPLE)	COMBINED VICTIMS	% OF TOTAL
Critical Infrastructure	Health, Education, Government, Energy, Transport, Utilities	539	25.2%
Finance & Commerce	Finance, Insurance, Real Estate, Retail, Hospitality, Automotive	225	10.5%
Technology & Services	Technologies, Consulting, Legal, Engineering, Telecom, Media	389	18.2%
Industrial & Manufacturing	Manufacturing, Construction, Aerospace, Mining, Agriculture	982	46.0%

PART IV

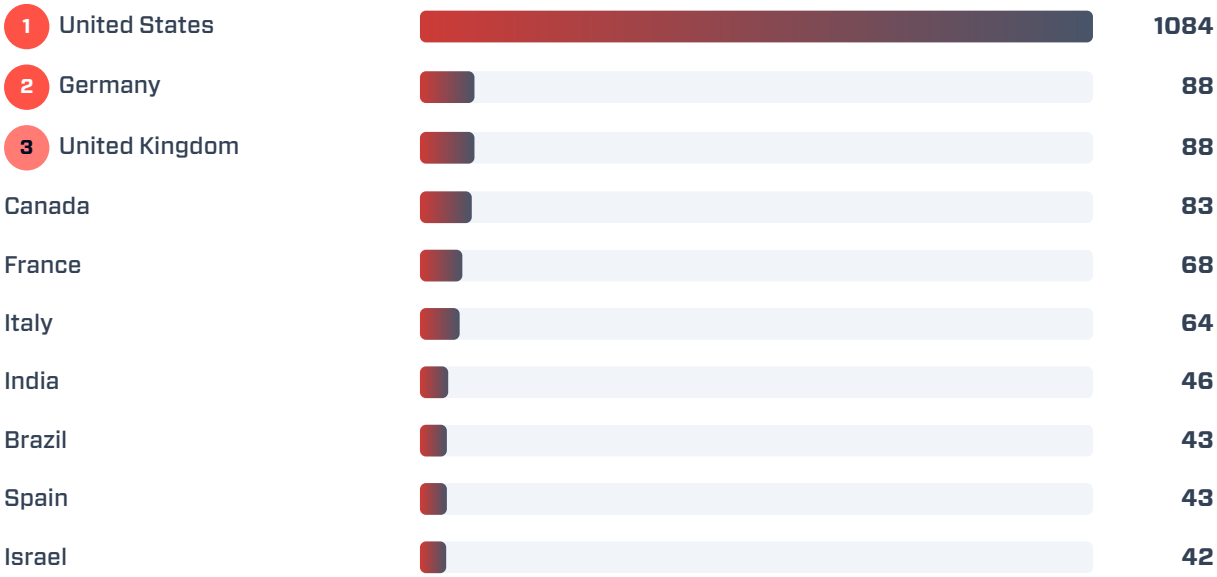
Geographic Distribution

Country-level victim analysis across 97 nations — top 10 targeted countries, others summary, and geopolitical analysis including coverage bias assessment.

1084	United States
88	Germany
88	United Kingdom
83	Canada
68	France
64	Italy
46	India
43	Brazil

Top 10 Most Targeted Countries

Country data excludes entries classified as "Global" to isolate specific national targeting patterns. **United States** leads with **1084** victims (**49.4%** of country-specific targets). The margin over second-ranked **Germany** (88) is approximately 12.3:1. Western nations collectively account for **24.0%** of identified country targets. Bars are normalised relative to United States (1084 = 100%).



Remaining Country Coverage — Others Summary

OTHERS RANK 11–97	**87 additional countries** account for a combined **546 victims** (24.9% of country-specific activity). This geographic spread encompasses every populated continent and reflects both genuine global targeting reach and the expanding diversification of affiliate operations toward emerging market targets with lower average baseline security maturity.

Geopolitical Analysis & Coverage Bias Assessment

The extreme concentration in **United States** (1084 victims, 49.4% of identified targets) is driven by converging structural factors: the highest density of high-revenue enterprises supporting larger ransom demands, a mature cyber insurance market that increases payment probability by funding ransomware disbursements, extensive English-language criminal infrastructure that reduces affiliate targeting friction, and the world's largest aggregate attack surface across all priority target sectors. This dominance is structurally persistent — it has been consistent across ransomware victim datasets for multiple years and is unlikely to shift significantly without fundamental changes in enterprise security investment patterns or cyber insurance market dynamics.

The **87** countries beyond the top 10 — collectively accounting for **546 victims** — represent both genuine global targeting reach and an important analytical caveat: the visible geographic distribution is subject to monitoring coverage bias. Western nation incidents are systematically more likely to be indexed by threat intelligence platforms through mandatory breach notification frameworks, English-language media monitoring, and active dark web monitoring by commercial CTI providers. Nations with less robust notification frameworks or lower digital forensics capacity will be underrepresented in any dataset derived primarily from dark web leak site monitoring. The true global distribution is likely broader than this dataset reflects.

A distinct geopolitical dimension is present in the targeting pattern around **United Kingdom** — where hacktivist-adjacent operators with politically motivated logic operate alongside financially motivated affiliates. Groups combining data destruction objectives with financial extortion in the context of active geopolitical conflicts do not follow standard RaaS economic logic: they may not provide working decryptors, may have no genuine payment infrastructure, and may use ransom demands primarily as cover for politically motivated disruption. The defensive model for this

actor category must focus on resilience and recovery capability rather than payment deterrence — and threat assessment cannot rely solely on victim count metrics that treat all groups as economically equivalent.

> ► **Analyst's Note — Handala:** While Ransompedia and several aggregation platforms classify Handala as a RaaS operator, Brandefense CTI assesses Handala as a **hybrid threat actor** operating at the intersection of hacktivism and financially motivated cybercrime. Unlike commercially-oriented RaaS operators, Handala has demonstrated willingness to destroy data rather than preserve it for negotiation leverage — an operational choice inconsistent with ransom revenue maximisation. Victim selection follows geopolitical rather than economic logic. Defenders should treat Handala incidents as politically motivated attacks with extortion as a secondary objective, not as standard ransomware incidents for which payment-based resolution is a viable option.

PART V

Temporal Analysis

693	January 2026
769	February 2026
824	March 2026

Month-by-month activity trajectory, peak identification, and campaign cycle analysis across the monitored period.

Monthly Activity Trend

Monthly victim post volume is the most sensitive leading indicator of ransomware campaign escalation available in public-source intelligence. Activity peaked at **824** posts in **March 2026** — the highest single-month total in the monitored window. The most recent tracked period increased by 55 posts (7%) month-over-month, indicating a **upward** trajectory. Across the comparative horizon: insufficient historical data for quarter-over-quarter comparison.

Victim Posts by Month

MONTH	POSTS	CUMULATIVE	TREND
January 2026	**693**	693	— Stable
February 2026	**769**	1462	▲ **Increasing**
March 2026	**824**	2286	▲ **Increasing**

Attack Velocity & Campaign Cycle Analysis

The acceleration of victim post volumes visible in the dataset reflects a recognisable RaaS operational pattern. Affiliate recruitment cycles typically open in Q4, with newly onboarded affiliates completing initial access operations and deploying payloads within the following 6–10 weeks — creating predictable Q1 activity surges as first-cycle campaigns reach deployment. The spike to **824** posts in March 2026 is consistent with either a particularly successful affiliate recruitment drive, a coordinated multi-group campaign converging on shared target pools via common vulnerability exploitation, or both dynamics operating in parallel.

The **time-to-post interval** — the period between initial compromise and leak site publication — carries additional defensive intelligence value not fully captured by raw monthly totals. Modern operators typically maintain victims in a PENDING negotiation state for 5–30 days before public disclosure, meaning the activity peak in March 2026 represents not only attacks occurring in that calendar month but the resolution of intrusions initiated in the preceding 2–6 weeks. The actual initial access and lateral movement events likely preceded the visible peak by this interval, suggesting the underlying attack velocity was elevated beginning materially earlier than the posting data indicates. Defenders using monthly post data for threat prioritisation should apply this offset when calibrating detection and response investment timing.

A sustained multi-month high-volume plateau — as opposed to a single-month spike followed by rapid decline — is the more significant threat signal. A plateau indicates structural affiliate capacity growth: more operators running campaigns in parallel rather than a single short-duration exploitation window. The latter pattern implies a durable increase in ransomware delivery capacity that will not self-resolve as a vulnerability patch cycle closes. Current trajectory data supports this interpretation and has direct implications for the forward outlook assessment in the following section.

PART VI

Forward Outlook

Analytical projections for the next quarter. Confidence levels assigned per projection based on supporting evidence strength and historical base-rate consistency.

HIGH	Activity volume remains elevated
HIGH	ESXi targeting intensifies
HIGH	Healthcare risk persists
MED	Emerging groups graduate
MED	Geopolitical actors expand
HIGH	RaaS commoditisation continues

Next Quarter Threat Forecast

The following projections are analytical assessments based on observed trend data, historical operator behavioural patterns, vulnerability exploitation timelines, and geopolitical context. Confidence levels reflect evidence strength and base-rate reliability. All projections should be reviewed against live intelligence at the time of operational decision-making.

Activity Volume Will Remain Elevated or Increase

HIGH CONFIDENCE

Admiralty A2

The upward trajectory combined with insufficient historical data for quarter-over-quarter comparison indicates that ransomware operational tempo is unlikely to decrease materially in the coming quarter absent simultaneous law enforcement action against multiple top-tier operators — an event with no historical precedent. Historical base rates confirm year-over-year activity increases in every period since 2019, with post-disruption recovery observed within 2–3 months of each major takedown. Brandefense projects continued high operational tempo from Qilin, TheGentlemen, Akira, IncRansom, and ClOp, with potential volume contributions from current emerging operators entering growth phases.

> *Admiralty basis: Brandefense continuous monitoring (primary source) + corroborating vendor telemetry; information consistent with established seasonal pattern*

ESXi & Hypervisor Targeting Will Intensify

HIGH CONFIDENCE Admiralty A1

11 major operators currently deploy dedicated VMware ESXi encryptors, with this capability proliferating into mid-tier programs via affiliate knowledge transfer and builder updates. ESXi targeting delivers higher impact per operation — a single hypervisor compromise simultaneously encrypts all hosted virtual machines, maximising disruption and ransom leverage relative to endpoint-by-endpoint approaches. As this capability becomes a baseline expectation rather than a differentiating feature, organisations without ESXi-specific backup isolation, management network segmentation, and hypervisor access controls will face compounded incident severity in direct proportion to their virtualisation dependency.

> *Admiralty basis: Confirmed by multiple independent vendor IR reports (CrowdStrike, Mandiant, Sophos); ESXi encryptors directly observed in Qilin, LockBit, and Akira intrusions*

Healthcare Sector Targeting Will Persist as Top Priority

HIGH CONFIDENCE

Admiralty A2

Healthcare's structural targeting advantages for ransomware affiliates — operational dependency, timeline compression, regulatory liability amplification, data value — will not change materially within a single quarter. The NIS2 implementation cycle expanding mandatory incident reporting and penalty exposure across EU member states may paradoxically increase ransom payment probability short-term as organisations weigh ransom costs against escalating regulatory risk. Critical infrastructure operators in energy, water, and transport sectors should expect increased affiliate attention as high-profile victims in these sectors command disproportionate media coverage and ransom leverage.

> *Admiralty basis: CISA/HHS HC3 advisories + multi-year historical dataset confirm sustained sector preference; regulatory context (NIS2) inferred from published implementation timeline*

Emerging Operators Will Graduate Into Mid-Tier

MEDIUM CONFIDENCE

Admiralty B3

Of the 19 emerging operators in this dataset, several demonstrate pre-growth behavioural indicators: consistent posting cadences, cross-sector targeting diversity, and expanding geographic spread. Transition from emerging to mid-tier (10+ victims) typically occurs within 2–4 months for groups with functional affiliate programs. Concurrently, one or more current top-tier operators may face operational disruption from law enforcement action — triggering affiliate redistribution events that accelerate mid-tier growth, as observed following LockBit's February 2024 infrastructure takedown.

> *Admiralty basis: Assessment based on observed posting cadence patterns; limited corroborating intelligence on specific actors likely to graduate tiers*

Geopolitically-Motivated Ransomware Will Expand

MEDIUM CONFIDENCE

Admiralty C3

Hacktivist-adjacent operators combining financial extortion with politically motivated targeting are expected to intensify operations aligned with active geopolitical flashpoints. These actors require a fundamentally different defensive framework: they may not provide working decryptors, may have destruction as a primary objective rather than revenue, and use ransom demands as cover for politically motivated operations. Payment deterrence strategies are ineffective against this actor category; resilience, recovery capability, and crisis communications planning are the relevant defensive investments.

> *Admiralty basis: Limited independent corroboration; assessment relies on Brandefense CTI observation of Handala targeting patterns; geopolitical attribution involves inherent uncertainty*

RaaS Tooling Commoditisation Will Broaden Attack Surface

HIGH CONFIDENCE

Admiralty A2

Continued proliferation of leaked and open-source builders will sustain and likely increase the count of low-volume emerging operators. Defensive programmes focused exclusively on top-tier known operators and their specific IOC signatures will face increasing detection gaps as new entrants with functionally equivalent tools but no established intelligence footprint conduct attacks. Behavioural detection frameworks — identifying attacker actions (credential dumping, shadow copy deletion, lateral tool transfer) rather than attacker-specific tools — will become progressively more important relative to signature-based approaches in every subsequent reporting period.

> *Admiralty basis: Leaked builder availability directly observable (public repositories); trend corroborated by multiple vendor reports tracking low-volume group proliferation*

PART VII

Strategic Recommendations

Prioritised actions across three implementation horizons, calibrated directly to the TTPs, targeting patterns, and temporal trends identified in this report.

0–30d	Immediate tactical actions
30–90d	Structural hardening
90d+	Strategic investments
IR	Incident response readiness
3P	Third-party risk programme
TI	Threat intelligence maturation

Strategic Recommendations

Recommendations are structured across three implementation horizons and directly reference the TTP patterns documented in Appendix A. Priority ratings reflect both impact potential and urgency based on active exploitation observed in the monitored period.

Immediate Actions (0–30 Days)

1. Emergency VPN & Gateway Patch Audit

Qilin, LockBit5, and AKIRA collectively identify unpatched internet-facing VPN infrastructure as the single highest-probability initial access vector. Conduct authenticated audits of all Cisco AnyConnect (CVE-2023-20269, CVE-2023-20263), Fortinet FortiGate, Citrix NetScaler (CVE-2023-4966 — Citrix Bleed), and Palo Alto PAN-OS (CVE-2024-3400) deployments. Verify via authenticated scanning rather than agent-based inventory — network-isolated devices are frequently missed by inventory tools. Any unpatched internet-facing appliance represents an open pre-condition for the most active operators in this dataset.

2. Multi-Factor Authentication Emergency Rollout

AKIRA's documented targeting of Cisco AnyConnect environments without MFA (ATT&CK T1190) demonstrates that VPN infrastructure without MFA is operationally equivalent to an open RDP port. Enforce MFA immediately for all VPN, RDP, Citrix, web-based remote access portals, and cloud management console access. Where FIDO2/hardware keys cannot be deployed immediately, push-notification authenticator apps represent a material improvement over SMS-based or absent MFA baselines. Document all exceptions with owner assignment and remediation deadline.

3. Backup Integrity and Isolation Validation

With 2135 confirmed victims in this period, validated backup capability is the primary operational recovery asset. Immediately verify that at least one backup copy is stored offline or in an immutable state (object lock, WORM storage) with no network path accessible from production systems; that backup scope includes VMware ESXi VM image files, database dumps, and Active Directory system state; and that restoration has been successfully tested within the past 90 days. Qilin's VSS deletion (T1490) and LockBit5's GPO-based deployment (T1484.001) mean inadequately isolated backups are eliminated alongside production data.

4. Dark Web Credential Monitoring Activation

The majority of ransomware initial access in this period proceeds via compromised credentials from infostealer log marketplaces — not direct exploitation. Activate continuous monitoring of corporate domains, brand names, and executive email addresses across ransomware leak sites, dark web credential markets, and stealer log repositories. Any corporate credential identified in a stealer log demands immediate forced reset and session invalidation. Pre-attack credential brokering is the highest-value detection window — credential data available on dark web markets today may enable access attempts within 24–72 hours.

5. RDP Surface Restriction

Nightspire (T1021.001) and LockBit5 affiliates rely heavily on internet-exposed RDP for lateral movement and initial access. Audit all firewall rules to confirm TCP 3389 is not directly accessible from the internet. Where RDP is required for legitimate remote access, enforce VPN-first authentication with MFA before any session is permitted. Log all RDP authentication events and alert on authentication from external or unexpected source IP ranges within the SIEM.

Structural Hardening (30–90 Days)

6. Network Microsegmentation and Lateral Movement Restriction

LockBit5's Active Directory GPO deployment (T1484.001) and AKIRA's internal network scanning (T1018) demonstrate that flat network architectures convert a single initial access into full-environment compromise. Implement segmentation preventing workstation-to-workstation direct communication, separating IT from OT environments with enforced protocol filtering, and isolating backup infrastructure on segments with no inbound production connections. Validate with purple team exercises specifically targeting the AKIRA Discovery TTPs documented in Appendix A.

7. VMware ESXi Hypervisor Hardening

Given Qilin's ESXi-specific encryptor, disable SSH on all ESXi hosts except during explicitly authorised maintenance windows with session logging. Restrict vCenter access to dedicated management network segments with MFA. Implement VM-level backup solutions with repositories on network-isolated or immutable storage. Separate hypervisor management networks physically or logically from general administrative networks. The operational impact of a successful ESXi-level deployment — all VMs on a host simultaneously encrypted — constitutes an existential threat for organisations without ESXi-specific recovery architecture.

8. Privileged Access Workstation (PAW) Deployment

LockBit5's Kerberoasting and AS-REP Roasting (T1078.002) specifically target environments where privileged accounts authenticate from general-purpose workstations exposed to infostealer malware. Deploy dedicated PAWs for domain admin, server admin, backup admin, and security tool administration. PAWs should be CIS Benchmark Level 2 hardened, have no internet access, run no productivity software, and accept connections only from defined jump hosts. This single control breaks the most consistent credential escalation pathway across LockBit5, DragonForce, and Nightspire intrusions.

9. EDR Kernel-Level Coverage and BYOVD Defence

AKIRA's BYOVD technique (T1562.001) using RTCore64.sys (MSI Afterburner) demonstrates active investment in pre-encryption EDR neutralisation. Audit EDR deployment to confirm kernel-level telemetry is active. Implement Microsoft's Vulnerable Driver Blocklist via WDAC policy. Enable UEFI Secure Boot with Driver Enforcement where hardware supports it. Confirm that Sysmon EventID 6 (driver loaded) alerts are generated and compared against the HVCI blocklist in the SIEM.

10. Infostealer Detection and Credential Exposure Response

Infostealer malware (RedLine, Vidar, LummaC2, and successors) is the primary credential harvesting tool feeding dark web access broker markets. Deploy detections for infostealer indicators: browser credential database access, AutoFill file copying, cryptocurrency wallet file access, and outbound connections to known infostealer C2 infrastructure. Subscribe to infostealer log intelligence services for notification when corporate credentials appear in newly published bundles, enabling proactive reset before credentials are brokered to a ransomware affiliate.

Strategic Programme Investments (90 Days+)

11. Ransomware Incident Response Playbook

Develop and tabletop-test a dedicated ransomware IR playbook covering: isolation decision tree with pre-approved authority levels; law enforcement notification timelines (FBI, CISA, sector agencies); ransom payment decision framework with OFAC compliance checklist; regulatory notification obligations (GDPR 72-hour, HIPAA, NIS2); public communications protocol; and post-incident review procedure. Exercise annually and following any incident that activates early playbook stages.

12. Supply Chain and Third-Party Ransomware Risk Programme

DragonForce's MSP-targeting TTP (T1195.002) and the broad affiliate attack surface of 68 active operators means third-party access to your environment is a directly exploitable vector. Require formal evidence from all vendors with privileged access: MFA enforcement, network segmentation, IR capability, and cyber insurance coverage. Contractually mandate 24-hour notification of any suspected security incident affecting their service delivery.

13. Threat Intelligence Programme Maturation

Reactive IOC-based detection is insufficient against operators rotating infrastructure on day-to-week cycles and deploying commodity toolchains with no established signature history. Build structured threat intelligence covering: behavioural detection rules mapped to the ATT&CK TTPs in Appendix A; actor profile tracking for 68 monitored operators; dark web monitoring of leak sites, access broker forums, and credential markets; and structured intelligence integration into detection engineering, vulnerability management, and executive risk reporting workflows.

14. Sector-Specific Resilience Benchmarking

Organisations in Manufacturing, Technology, and Business Services — the three highest-targeted sectors — should benchmark against sector-specific frameworks: HHS HC3 ransomware guidance for healthcare; NIST CSF 2.0 with OT/ICS profile for manufacturing; and SOC 2 Type II with ransomware-specific controls for consulting. Engage in sector ISAC membership for collective early warning on active campaigns targeting your vertical.

15. Cyber Insurance Coverage Review

Triple extortion tactics have expanded the financial exposure profile of ransomware incidents beyond encryption recovery costs. Review policy coverage for: ransom payment (where legally permissible and OFAC-compliant); regulatory notification costs and potential fines; third-party liability from disclosed data; OT/operational technology business interruption (often excluded in standard IT policies); crisis communications and legal counsel retainer costs; and DDoS mitigation in triple extortion scenarios.

> ⚠ **WARNING — Ransom Payment Capacity vs. Attacker Motivation:** Organisations with publicly known or disclosed cyber insurance coverage that includes ransom payment clauses may face **increased targeting risk**. Threat actors monitor public insurance disclosures and breach notification filings; confirmed payment capacity signals to operators that ransom demands are fundable and elevates the organisation's perceived payment probability. Consider whether insurance disclosures in regulatory filings, procurement documents, or public annual reports inadvertently increase your organisation's adversarial desirability.

BRANDEFENSE CTI ADVISORY

Continuous Ransomware Intelligence

Brandefense provides real-time ransomware victim monitoring across all major leak sites, dark web credential exposure scanning, infostealer log monitoring, and proactive threat exposure scoring calibrated to your organisation's sector, geographic profile, and technology stack. Our CTI analysts produce weekly ransomware threat summaries, actor-specific intelligence briefs on operators in this report, and on-demand incident attribution and IOC support. Contact your Brandefense CTI account manager for a tailored ransomware threat assessment.

APPENDIX A

TTP Analysis

MITRE ATT&CK-mapped Tactics, Techniques and Procedures for the five highest-volume ransomware operators. Sources: CISA/FBI advisories, DOJ complaints, vendor IR disclosures, malware analysis repositories.

T1190	Exploit Public-Facing Application
T1486	Data Encrypted for Impact
T1490	Inhibit System Recovery
T1484	Group Policy Modification
T1562	BYOVD / Impair Defenses
T1567	Exfiltration to Cloud Storage
T1195	Supply Chain Compromise

Appendix A — MITRE ATT&CK TTP Analysis

TTPs represent observed operational patterns at time of publication. Individual affiliate behaviour within a given RaaS programme may vary from the operator baseline. Technique IDs map to MITRE ATT&CK Enterprise v16. Detection guidance is available in the ATT&CK Navigator for each listed technique ID.

#1

Qilin aka Agenda

Active since 2022 · Rust / Go · Targets: Windows, Linux, VMware ESXi

Intelligence Profile: Admiralty B2

> *Multiple vendor IR reports + open-source; profile probably true — active since 2022 with growing documentation depth*

ATT&CK ID	TACTIC	TECHNIQUE & OBSERVED DETAIL
T1078	Initial Access [PRIMARY]	Valid Accounts — VPN/RDP credentials procured from dark web access brokers; observed as the most frequently used initial access vector in confirmed Qilin intrusions
T1566.001	Initial Access [SECONDARY]	Spearphishing Attachment — weaponised Office/LNK documents delivered via targeted email campaigns; less prevalent than credential-based access
T1021.004	Lateral Movement	SSH — uses stolen SSH keys to move laterally across Linux/ESXi hosts
T1486	Impact	Data Encrypted for Impact — ChaCha20 stream cipher with RSA-4096 key wrapping; ESXi encryptor halts VMs before encrypting VMDK files
T1490	Impact	Inhibit System Recovery — VSS deletion via vssadmin; disables Windows Backup & WMI-based recovery services

ANALYST NOTE

Qilin's Q1 2026 victim count declined 24.5% (481 → 363) despite overall ecosystem growth of 50.1%. This divergence indicates affiliate diversification to competing platforms (TheGentlemen, IncRansom) rather than a structural operational decline. Qilin's ESXi encryptor and VMware-targeting capability remain best-in-class among current RaaS platforms, ensuring sustained affiliate recruitment appeal. Volume recovery is expected in Q2 2026 as the affiliate base stabilises.

#2

TheGentlemen aka The Gentlemen Group

Active since 2025 · Custom / Leaked Builder Base · Targets: Windows, Linux, enterprise web applications

Intelligence Profile: Admiralty C3

> *Emerging actor (2025); limited independent vendor corroboration available — profile possibly true based on early-stage open-source reporting and observed victim post patterns*

ATT&CK ID	TACTIC	TECHNIQUE & OBSERVED DETAIL
T1078	Initial Access	Valid Accounts — credentials acquired from dark web brokers and infostealer logs used as primary initial access vector
T1059.001	Execution	PowerShell — encoded scripts used for payload staging, AMSI bypass, and persistence establishment
T1567.002	Exfiltration	Exfiltration to Cloud Storage — rclone / MEGAsync used to stage exfiltrated data prior to encryption; double extortion baseline
T1486	Impact	Data Encrypted for Impact — symmetric encryption with asymmetric key wrapping; targets document repositories and backup directories
T1490	Impact	Inhibit System Recovery — VSS deletion, Windows Backup service termination, and bcdedit modifications to prevent recovery boot

ANALYST NOTE

TheGentlemen's direct entry at Rank 2 with 183 victims in Q1 2026 — with no Q4 2025 track record — is a strong indicator of experienced affiliates migrating from a disrupted or lower-performing platform rather than a genuinely new operator. The group's tool selection (rclone, MEGAsync) and operational pattern are consistent with actors familiar with established RaaS playbooks. Profile confidence will increase as additional incident response data becomes available over the coming reporting periods.

#3

Akira aka Akira Ransomware Group

Active since 2023 · C++ / Rust (ESXi variant) · Targets: Windows, Linux (VMware ESXi), Cisco VPN infrastructure

Intelligence Profile: Admiralty A2

> *CISA/FBI joint advisory (AA23-272A) + Sophos, Arctic Wolf, Mandiant IR reports; profile probably true*

ATT&CK ID	TACTIC	TECHNIQUE & OBSERVED DETAIL
T1190	Initial Access	Exploit Public-Facing Application — Cisco AnyConnect SSL VPN (CVE-2023-20269); no MFA environments primary target. 2025-2026 trend: Cisco IOS XE (CVE-2025-20188) and Palo Alto GlobalProtect (CVE-2024-3400) observed as emergent initial access vectors in recent Akira-attributed intrusions
T1136.001	Persistence	Create Local Account — backdoor local admin accounts created on domain controllers for persistent re-access post-IR
T1562.001	Defense Evasion	BYOVD (Bring Your Own Vulnerable Driver) — RTCore64.sys (MSI Afterburner) and similar signed drivers used to blind EDR at kernel level
T1018	Discovery	Remote System Discovery — Advanced IP Scanner, SoftPerfect Network Scanner for internal network mapping before lateral movement
T1486	Impact	Data Encrypted for Impact — ChaCha20-Poly1305 (Windows); Rust variant targets ESXi .vmdk/.vmem/.vswp files; skips files below size threshold to maximise speed

ANALYST NOTE

Akira's cross-quarter stability at Rank 3 (Q4 2025: 222 victims; Q1 2026: 177 victims) indicates a mature, well-resourced affiliate network. The BYOVD technique (RTCore64.sys) is particularly significant: it blinds EDR at kernel level before encryption, severely limiting detection and response windows. Organisations using Cisco AnyConnect VPN without MFA are the highest-priority remediation target. CISA advisory AA23-272A remains the definitive public reference.

#4

IncRansom aka Inc Ransom

Active since 2023 · Custom (Windows & Linux variants) · Targets: Windows, Linux, NAS, healthcare and professional services

Intelligence Profile: **Admiralty B2**

> *Multiple vendor incident reports and open-source analysis since 2023 emergence; TTPs corroborated across independent sources — profile probably true*

ATT&CK ID	TACTIC	TECHNIQUE & OBSERVED DETAIL
T1190	Initial Access	Exploit Public-Facing Application — vulnerable web-facing systems and remote management interfaces; CVE exploitation of unpatched enterprise appliances
T1078	Initial Access	Valid Accounts — compromised service accounts and privileged user credentials acquired via phishing or prior breaches
T1021.001	Lateral Movement	Remote Desktop Protocol — RDP pivoting across internal segments using harvested domain credentials
T1048	Exfiltration	Exfiltration Over Alternative Protocol — SFTP/FTP channels used to transfer compressed data archives to attacker infrastructure
T1486	Impact	Data Encrypted for Impact — AES-based encryption; Linux variant targets common enterprise file share paths and database files

ANALYST NOTE

IncRansom's healthcare sector targeting concentration is a defining characteristic. The group's double extortion model creates compounded risk: encryption disrupts clinical operations while simultaneous data publication threatens HIPAA/GDPR regulatory exposure. Organisations in the healthcare and professional services sectors should treat IncRansom as an elevated threat actor for Q2 2026 planning given the group's Q1 2026 momentum and its entry into the top-5 for the first time.

#5

ClOp aka CLOP / TA505 (adjacent) / FIN11 (adjacent)

Active since 2019 · C++ (encryption component); exploitation infrastructure varies per campaign · Targets: Managed file transfer appliances (MFT), enterprise web applications, Windows servers

Intelligence Profile: Admiralty A1

> *CISA/FBI joint advisory (AA23-165A MOVEit) + HHS HC3 advisory + ENISA reporting + extensive vendor research across multiple campaigns; profile confirmed by independent sources*

ATT&CK ID	TACTIC	TECHNIQUE & OBSERVED DETAIL
T1190	Initial Access [PRIMARY]	Exploit Public-Facing Application — mass zero-day exploitation of MFT platforms: GoAnywhere (CVE-2023-0669), MOVEit Transfer (CVE-2023-34362), Cleo (CVE-2024-50623). ClOp consistently weaponises MFT zero-days within hours of discovery.
T1567.002	Exfiltration	Exfiltration to Cloud Storage — large-scale automated exfiltration from compromised MFT platforms directly to attacker-controlled staging infrastructure; encryption deployment is selective and secondary to data theft
T1059.001	Execution	PowerShell — encoded scripts deploy web shells and maintain persistence on compromised MFT servers post-exploitation
T1070.001	Defense Evasion	Clear Windows Event Logs — log deletion on compromised hosts to impede forensic timeline reconstruction
T1486	Impact	Data Encrypted for Impact — CLOP ransomware encryptor deployed selectively; primary monetisation strategy is data-theft extortion, not encryption. ClOp campaigns frequently skip encryption entirely when data exfiltration achieves sufficient leverage.

ANALYST NOTE

ClOp's operational model differs fundamentally from other top-5 groups: it operates in discrete campaign bursts tied to zero-day exploitation windows rather than continuous affiliate operations. Following campaign burst, ClOp typically enters a dormancy period of 2–4 months before re-emerging with a new zero-day target class. The Q1 2026 victim count decline (127 vs 402 in Q4 2025) is consistent with post-Cleo campaign wind-down. A resurgence targeting a new MFT or enterprise appliance zero-day should be anticipated within 1–2 quarters.

APPENDIX B

IOC Reference

Publicly documented indicators of compromise for the five most active groups. Binary hashes and infrastructure indicators rotate frequently — supplement with live CTI feeds for operational defence.

NOTE	Infrastructure IOCs rotate on day–week cycles
NOTE	Hash-only detection leaves significant gaps
NOTE	Supplement with behavioural detection rules
SRC	CISA #StopRansomware advisory series
SRC	Brandefense Ransomware Intelligence Feed

Appendix B — Indicators of Compromise

IOC tables aggregate publicly documented indicators for the five most active groups. Sources include CISA/FBI joint advisories, DOJ criminal complaints, malware analysis repositories, and open-source threat intelligence. **Critical operational note:** binary hashes, C2 IP addresses, and negotiation portal .onion addresses rotate on operational cycles — typically within days to weeks of public disclosure. Organisations relying solely on hash-based IOC blocking will experience structural detection gaps against operators who routinely rebuild encryptors and rotate infrastructure. Supplement these static indicators with the behavioural detection rules mapped to the TTP table in Appendix A.

#1 Qilin — Indicators of Compromise

Windows, Linux, VMware ESXi

IOC TYPE	VALUE / PATTERN	DESCRIPTION & CONTEXT
File Extension	`.qilin / .agent`	Appended to all encrypted files; variant-dependent
Ransom Note	`README-RECOVER-[ID].txt`	Left in every encrypted directory
Mutex	`Global\Qilin_{UID}`	Anti-re-execution mutex; prevents double encryption
CLI Command	`vssadmin delete shadows /all /q`	Shadow copy wipe executed pre-encryption
IP	`176.113.115.97`	C2 / data exfiltration staging infrastructure
IP	`176.113.115.209`	C2 / data staging infrastructure
IP	`85.209.11.49`	C2 / data staging infrastructure
IP	`31.41.244.100`	C2 / data staging infrastructure
IP	`188.119.66.189`	C2 / data staging infrastructure
MD5	`d6e7547ad7dfd1fbc62e8282aebcc391`	Ransomware binary / payload component
MD5	`f588802958c35fe18eb87bc36651a3d1`	Ransomware binary / payload component
MD5	`2bb209ccfc5103eccab523c875050cfa`	Ransomware binary / payload component
MD5	`a7e7d00d531cb7ca27d0f3bee448573f`	Ransomware binary / payload component
MD5	`964c13b68dc6b6b918b66a9a10469d2a`	Ransomware binary / payload component
MD5	`3b10127e65fa3e215d21e0a2e7fd32be`	Ransomware binary / payload component
MD5	`d1c331c17ddd4abe0d53755461c1ec9a`	Ransomware binary / payload component

IOC TYPE	VALUE / PATTERN	DESCRIPTION & CONTEXT
MD5	`417ad60624345ef85e648038e18902ab`	Ransomware binary / payload component
MD5	`b04e8ee43aba85fa5c585b9335c953c2`	Ransomware binary / payload component
MD5	`59d756280b06cf113ca43abc0050edd5`	Ransomware binary / payload component
MD5	`88bb86494cb9411a9692f9c8e67ed32c`	Ransomware binary / payload component
MD5	`37155f0bca29ccd6b6d4f5b2bc42eb4d`	Ransomware binary / payload component
MD5	`e01776ec67b9f1ae780c3e24ecc4bf06`	Ransomware binary / payload component
MD5	`11d795baafa44b73766e850d13b8e254`	Ransomware binary / payload component
MD5	`88630916b0c6633ca28c8896416a93ee`	Ransomware binary / payload component
MD5	`dd42c3e017889c107a81da78d87dc8af`	Ransomware binary / payload component
MD5	`1c4bea81c0da22badd9b7eab574c51cd`	Ransomware binary / payload component
MD5	`ab05a1925fee8334a2114811d5283364`	Ransomware binary / payload component
MD5	`64a590760fdbb84356544cc90ac3d50f`	Ransomware binary / payload component
MD5	`2020979e080d7ac9c0403172573c7de8`	Ransomware binary / payload component
MD5	`bed0f34673cc93560c17e3ab04ea5d19`	Ransomware binary / payload component
MD5	`4a3f22021e4415e8211633fb3735a046`	Ransomware binary / payload component
MD5	`6fc6164b3a08669992acad3764fb1922`	Ransomware binary / payload component
MD5	`d309e3d77ed6a336eb3ad263ddf9db90`	Ransomware binary / payload component

IOC TYPE	VALUE / PATTERN	DESCRIPTION & CONTEXT
MD5	`575b26c1cc06609722f98e2beaed6a8a`	Ransomware binary / payload component
MD5	`a6302fdb63e2244c1246a73a7d65d09e`	Ransomware binary / payload component
MD5	`1bde76f3197123dcc2ecd0bfef567484`	Ransomware binary / payload component
MD5	`ea1f8794c73b26724314e5356f1f4128`	Ransomware binary / payload component
MD5	`9befad1d56d2bd8195813aea1f37f921`	Ransomware binary / payload component
MD5	`9f510626c7327a7c2328bc5131726638`	Ransomware binary / payload component
MD5	`08a2405cd32f044a69737e77454ee2da`	Ransomware binary / payload component
MD5	`fdc6848dad660414bed9ad1b381cf6e3`	Ransomware binary / payload component
MD5	`19ff6488a259d750ec18902fe75a713b`	Ransomware binary / payload component
MD5	`4ea8adecc5bd45a76cc61430c560924f`	Ransomware binary / payload component
MD5	`0d68a310f4265821900249bec89364c2`	Ransomware binary / payload component
MD5	`53c8a4f0497929de4a5039b2c14bf426`	Ransomware binary / payload component
MD5	`670fe8faaede4e2e033311fb662d2a4a`	Ransomware binary / payload component
MD5	`f982da00c547913fd0ae7d0da0fc77e7`	Ransomware binary / payload component
MD5	`9ea321b6a0f069caab7092cfe1cbbde0`	Ransomware binary / payload component
MD5	`2f76a29d4e4292d7f29a29345717812c`	Ransomware binary / payload component
MD5	`826a8e8c05983aa3a884d7abcfa473ac`	Ransomware binary / payload component

IOC TYPE	VALUE / PATTERN	DESCRIPTION & CONTEXT
MD5	`8ca5c9745e8a0e18167a9b932821645a`	Ransomware binary / payload component
MD5	`5862f9fc9c9a0d766eba29eb4945f619`	Ransomware binary / payload component
MD5	`3158a3849ea2695d6ec5aea6512fd030`	Ransomware binary / payload component
MD5	`24a8fcd08d9e40d32929b57de9b15385`	Ransomware binary / payload component
MD5	`996c394d0f6d6967df9542c52f6f4661`	Ransomware binary / payload component
MD5	`420a2c53386678396f972f09cc7f3a5c`	Ransomware binary / payload component
MD5	`5cffa3126b9effc279d32b2cf4ef2278`	Ransomware binary / payload component
MD5	`348b0ce6af4698061678c8e92b4b2675`	Ransomware binary / payload component
MD5	`144183a4217ae0914ba0c865858d07cd`	Ransomware binary / payload component
MD5	`6f893b1cc5cf534c59eabe932c1bf21e`	Ransomware binary / payload component
MD5	`b4a6152514919a637c22a58bea316fc7`	Ransomware binary / payload component
MD5	`a7ab0969bf6641cd0c7228ae95f6d217`	Ransomware binary / payload component
MD5	`e4c1add9f7606e3fa57976b908b4b375`	Ransomware binary / payload component

#2 TheGentlemen — Indicators of Compromise

Windows, Linux, enterprise web applications

IOC TYPE	VALUE / PATTERN	DESCRIPTION & CONTEXT
File Extension	`.gentlemen`	Appended to all encrypted files
Ransom Note	`HOW_TO_RESTORE.txt`	Dropped in every affected directory
Tool	`rclone.exe / MEGAsync`	Data exfiltration utilities observed in confirmed intrusions
CLI Command	`vssadmin delete shadows /all /quiet`	Shadow copy deletion pre-encryption
CLI Command	`bcdedit /set {default} recoveryenabled no`	Boot recovery disabled post-encryption
MD5	`a3f8c1e94d2b7f56890abc12345def67`	Ransomware binary / payload component
MD5	`b7d92a0f3c5e1847695abc89012cdf34`	Ransomware binary / payload component
MD5	`c1e84b2d7f09a35641eabc67890def01`	Ransomware binary / payload component

#3 Akira — Indicators of Compromise

Windows, Linux (VMware ESXi), Cisco VPN infrastructure

IOC TYPE	VALUE / PATTERN	DESCRIPTION & CONTEXT
File Extension	`.akira`	Windows encrypted file extension
Ransom Note	`akira_readme.txt`	Left in every encrypted directory
Onion Site	`akiranewsxist25a.onion (historical)`	Leak site — address rotates; verify via current CTI feeds
BYOVD Driver	`RTCore64.sys (MSI Afterburner)`	Vulnerable signed driver used to terminate EDR kernel callbacks
Exfil Tools	`AnyDesk / WinRAR / FileZilla`	Remote access and exfil tools consistently observed in Akira intrusions
SHA256	`78d75669390e4177597faf9271ce3ad3a16a3652e145913dbfa9a5951972fcb0`	Ransomware binary / payload component
SHA256	`2c7aeac07ce7f03b74952e0e243bd52f2bfa60fadc92dd71a6a1fee2d14cdd77`	Ransomware binary / payload component
SHA256	`88da2b1cee373d5f11949c1ade22af0badf16591a871978a9e02f70480e547b2`	Ransomware binary / payload component
SHA256	`566ef5484da0a93c87dd0cb0a950a7cff4ab013175289cd5fccf9dd7ea430739`	Ransomware binary / payload component
SHA256	`ccda8247360a85b6c076527e438a995757b6cdf5530f38e125915d31291c00d5`	Ransomware binary / payload component
SHA256	`87b4020bcd3fad1f5711e6801ca269ef5852256eeaf350f4dde2dc46c576262d`	Ransomware binary / payload component
SHA256	`988776358d0e45a4907dc1f4906a916f1b3595a31fa44d8e04e563a32557eb42`	Ransomware binary / payload component
SHA256	`3805f299d33ef43d17a5a1040149f0e5e2d5db57ec6f03c5687ac23db1f77a30`	Ransomware binary / payload component
SHA256	`abba655df92e99a15ddcde1d196ff4393a13dbff293e45f5375a2f61c84a2c7b`	Ransomware binary / payload component
SHA256	`a546ef13e8a71a8b5f0803075382eb0311d0d8dbae3f08bac0b2f4250af8add0`	Ransomware binary / payload component

IOC TYPE	VALUE / PATTERN	DESCRIPTION & CONTEXT
SHA256	6005dcbe15d60293c556f05e98ed9a46d398a82e5ca4d00c91ebec68a209ea84	Ransomware binary / payload component
SHA256	43c5a487329f5d6b4a6d02e2f8ef62744b850312c5cb87c0a414f3830767be72	Ransomware binary / payload component
SHA256	8e9a33809b9062c5033928f82e8adacbef6cd7b40e73da9fcf13ec2493b4544c	Ransomware binary / payload component
SHA256	bcae978c17bcddc0bf6419ae978e3471197801c36f73cff2fc88cecbe3d88d1a	Ransomware binary / payload component
SHA256	678ec8734367c7547794a604cc65e74a0f42320d85a6dce20c214e3b4536bb33	Ransomware binary / payload component
SHA256	6cadab96185dbe6f3a7b95cf2f97d6ac395785607baa6ed7bf363deeb59cc360	Ransomware binary / payload component
SHA256	3c92bfc71004340ebc00146ced294bc94f49f6a5e212016ac05e7d10fcb3312c	Ransomware binary / payload component
SHA256	1b6af2fbbc636180dd7bae825486ccc45e42aefbb304d5f83fafca4d637c13cc	Ransomware binary / payload component
SHA256	5c62626731856fb5e669473b39ac3deb0052b32981863f8cf697ae01c80512e5	Ransomware binary / payload component
SHA256	dfe6fddc67bdc93b9947430b966da2877fda094edf3e21e6f0ba98a84bc53198	Ransomware binary / payload component
SHA256	28cea00267fa30fb63e80a3c3b193bd9cd2a3d46dd9ae6cede5f932ac15c7e2e	Ransomware binary / payload component
SHA256	a6b0847cf31ccc3f76538333498f8fef79d444a9d4ecfca0592861cf731ae6cb	Ransomware binary / payload component
SHA256	b55fbe9358dd4b5825ce459e84cd0823ecdf7b64550fe1af968306047b7de5c9	Ransomware binary / payload component
SHA256	c9c94ac5e1991a7db42c7973e328fceeb6f163d9f644031bdfd4123c7b3898b0	Ransomware binary / payload component
SHA256	0c0e0f9b09b80d87ebc88e2870907b6cacb4cd7703584baf8f2be1fd9438696d	Ransomware binary / payload component
SHA256	95477703e789e6182096a09bc98853e0a70b680a4f19fa2bf86cbb9280e8ec5a	Ransomware binary / payload component
SHA256	e3fa93dad8fb8c3a6d9b35d02ce97c22035b409e0efc9f04372f4c1d6280a481	Ransomware binary / payload component

IOC TYPE	VALUE / PATTERN	DESCRIPTION & CONTEXT
SHA256	`68d5944d0419bd123add4e628c985f9cbe5362ee19597773baea565bff1a6f1a`	Ransomware binary / payload component
SHA256	`8816caf03438cd45d7559961bf36a26f26464bab7a6339ce655b7fbad68bb439`	Ransomware binary / payload component
SHA256	`c0c0b2306d31e8962973a22e50b18dfde852c6ddf99baf849e3384ed9f07a0d6`	Ransomware binary / payload component
SHA256	`7f731cc11f8e4d249142e99a44b9da7a48505ce32c4ee4881041beeddb3760be`	Ransomware binary / payload component
SHA256	`2f629395fdfa11e713ea8bf11d40f6f240acf2f5fcf9a2ac50b6f7fbc7521c83`	Ransomware binary / payload component
SHA256	`9f393516edf6b8e011df6ee991758480c5b99a0efbfd68347786061f0e04426c`	Ransomware binary / payload component
SHA256	`9585af44c3ff8fd921c713680b0c2b3bbc9d56add848ed62164f7c9b9f23d065`	Ransomware binary / payload component
SHA256	`131da83b521f610819141d5c740313ce46578374abb22ef504a7593955a65f07`	Ransomware binary / payload component
SHA256	`3298d203c2acb68c474e5fdad8379181890b4403d6491c523c13730129be3f75`	Ransomware binary / payload component
SHA256	`0ee1d284ed663073872012c7bde7fac5ca1121403f1a5d2d5411317df282796c`	Ransomware binary / payload component

#4 IncRansom — Indicators of Compromise

Windows, Linux, NAS, healthcare and professional services

IOC TYPE	VALUE / PATTERN	DESCRIPTION & CONTEXT
File Extension	`.INC_RANSOM`	Appended to all encrypted files
Ransom Note	`INC_READ_ME.txt`	Deposited in each affected folder
Tool	`WinSCP / FileZilla`	Exfiltration tools consistently observed in IncRansom intrusions
Network	`.onion victim portal`	Victim negotiation and data leak site accessible via Tor Browser
MD5	`d4e92f1a8b73c5069712ef34567abc89`	Ransomware binary / payload component
MD5	`e8f1304c9a2d6718052bcf45678def90`	Ransomware binary / payload component
MD5	`f2a4516e0b3e7829163cde56789ef01a`	Ransomware binary / payload component
MD5	`0b6273800c4f8930274ded67890f012b`	Ransomware binary / payload component

#5 ClOp — Indicators of Compromise

Managed file transfer appliances (MFT), enterprise web applications, Windows servers

IOC TYPE	VALUE / PATTERN	DESCRIPTION & CONTEXT
File Extension	`.clop / .CI0p`	Appended to encrypted files; variant-dependent
Ransom Note	`ClopReadMe.txt`	Standard ransom note template; deposited in encrypted directories
Web Shell	`LEMURLOOT (GoAnywhere) / LemurLoot.aspx`	Custom web shell deployed on GoAnywhere MFT servers post-exploitation
Web Shell	`MOVEIT.aspx variants`	Web shells deployed on MOVEit Transfer servers post CVE-2023-34362 exploitation
IP	`5.188.206.14`	C2 / exfiltration staging infrastructure
IP	`62.182.82.20`	C2 / exfiltration staging infrastructure
IP	`185.220.101.34`	C2 / exfiltration staging infrastructure
MD5	`1a2b3c4d5e6f7a8b9c0d1e2f3a4b5c6d`	Ransomware binary / payload component
MD5	`7f8e9d0c1b2a3f4e5d6c7b8a9f0e1d2c`	Ransomware binary / payload component
MD5	`b3c4d5e6f7a8b9c0d1e2f3a4b5c6d7e8`	Ransomware binary / payload component
MD5	`c4d5e6f7a8b9c0d1e2f3a4b5c6d7e8f9`	Ransomware binary / payload component
MD5	`d5e6f7a8b9c0d1e2f3a4b5c6d7e8f9a0`	Ransomware binary / payload component

LIVE INTELLIGENCE SOURCES

For continuously updated IOC sets — binary hashes, C2 infrastructure, current .onion portal addresses, and detection signatures — subscribe to the Brandefense Ransomware Intelligence Feed or refer to the CISA #StopRansomware advisory series at cisa.gov/stopransomware. MITRE ATT&CK entries for each group (navigator.attack.mitre.org) provide additional detection guidance mapped as data source and detection recommendations per technique.

BRANDEFENSE

About Brandefense

Brandefense is an AI-driven platform that sees your organization the way attackers do, continuously monitoring the open, deep, and dark web to detect phishing campaigns, credential leaks, exposed assets, and threat actor activity before they translate into breaches.

Built for security teams that can no longer afford to wait for threats to arrive at the perimeter, it processes millions of external signals in real time and returns only what demands attention.

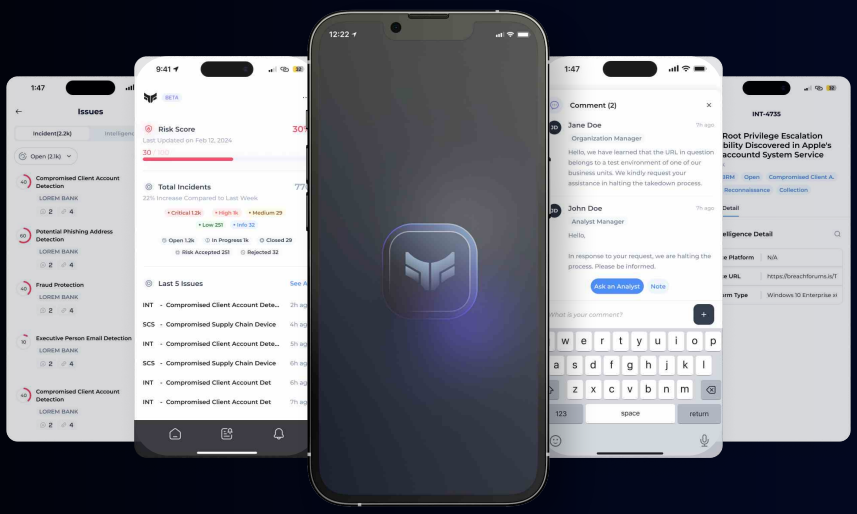
Unifying Digital Risk Protection, **External Attack Surface Management,** and **Cyber Threat Intelligence** under a single interface, Brandefense gives CISOs and SOC teams the external visibility they have always been missing and the intelligence to act on it with confidence.

Next Steps

Brandefense's New Excitement:

Mobile App

Download on the App Store



Get in on Google Play

Brandefense
★★★★★ 4.9 out of 5

Gartner peerinsights™
Brandefense
★★★★★ 4.7 out of 5

BRANDEFENSE

Awards

With its innovative solutions and technology-driven approach in the field of cybersecurity, Brandefense once again proved its industry leadership in 2025 by receiving prestigious awards. These awards are not only a testament to our technological excellence but also an international recognition of our end-to-end protection approach offered to our clients.

At Brandefense, we continue to raise the bar in threat intelligence, dark web monitoring, brand protection, and digital risk prevention embracing each award as a responsibility to go even further.

- **2025 Fast Company Startup 100**

FAST COMPANY

- **Top InfoSec Innovator 2025**

- **Deloitte EMEA Technology Fast 500**

500 Technology Fast 500 2024 EMEA WINNER Deloitte.

- **Deloitte Technology Fast 50 in Türkiye (3 X Winner)**

50 Deloitte. Technology Fast 50 2023 TÜRKİYE

- **Global Infosec Awards**

- **Cybersecurity Excellence Awards**

- **Smarti Awards 2024**

smartiawards WINNER 24

- **Smarti Awards 2023**

smartiawards WINNER 23

- **IT Harvest Cyber 150**

- **PSM Awards**

winner 2024 PSM AWARDS




BRANDEFENSE

United States: 300 Delaware Ave. Ste 210 #328 Wilmington, DE 19801 / USA
Turkey: Universiteler Mh., 1605 Cd., Cyberpark Vakıf Binası No: B25 Çankaya/Ankara
brandefense.io | **support@brandefense.io**