

Q U A R T E R L Y

RANSOMWARE

LANDSCAPE

REPORT



SECURITY OPERATIONS

Q1 2026 | JANUARY — MARCH

Delivering Actionable and Contextualized Intelligence to Increase Cyber Resilience

Table of Contents

1. Executive Summary
2. Key Performance Indicators
3. Monthly Trend Analysis
4. Most Active Ransomware Groups
5. Sector Analysis
6. Geographic Impact
7. Initial Access Vectors & Exploited CVEs
8. Notable Q1 2026 Campaigns
9. HACKURITY Threat Bulletins Issued
10. Strategic Outlook & Recommendations

1. Executive Summary

The first quarter of 2026 marked an alarming acceleration in global ransomware activity, with HACKURITY Threat Intelligence tracking **2,318 confirmed ransomware victims** across January through March—a sustained escalation over the previous quarter. The ransomware ecosystem demonstrated clear evolution: the dissolution of Black Basta following a catastrophic internal chat leak triggered a redistribution of experienced operators across rival groups, while new threat actors emerged with sophisticated supply chain attack methodologies.

HACKURITY currently monitors **385 ransomware and data extortion groups**, of which **270 maintain active leak sites** (online) and **115 are confirmed offline or dormant**. Q1 2026 saw consistent month-over-month growth in victim counts: **702 victims in January, 784 in February, and 832 in March**—representing a +18.5% increase from January to March.

The quarter was dominated by **Qilin** (370 victims), which cemented its position as the most prolific ransomware operation globally, absorbing talent and infrastructure from the dissolved Black Basta syndicate. **TheGentlemen** and **Akira** maintained aggressive campaigns with 186 and 185 victims respectively. The United States remained the primary target geography with 957 victims—representing 41% of all Q1 activity.

Key Intelligence Assessments

- > **Record Q1 Volume:** 2,318 victims across 3 months represents sustained high-tempo operations by ransomware syndicates, with March 2026 (832 victims) setting a new monthly record
- > **Black Basta Fragmentation:** The February 2026 internal leak precipitated the group's dissolution, spawning CipherForce and redistributing affiliates to Qilin, TheGentlemen, and other operations
- > **Supply Chain Escalation:** TeamPCP's multi-ecosystem campaign (GitHub/npm/PyPI/Docker Hub) combined with CipherForce's IDOR exploitation represents a new operational model—supply chain access weaponized for ransomware deployment
- > **European Cloud Targeting:** ShinyHunters' systematic breach of European enterprises and a major EU government institution (344GB exfiltrated) signals deliberate targeting of EU institutions and critical infrastructure
- > **HACKURITY published 10 threat bulletins** during Q1 2026, including flash alerts and advisories for sector-specific exposures

2. Key Performance Indicators



Quarter-over-Quarter Context

The Q1 2026 total of 2,318 victims reflects an increasingly industrialized ransomware ecosystem. The dissolution of Black Basta—once the fourth-largest operation—did not reduce overall victim counts but rather redistributed operational capacity to competing groups. Qilin’s absorption of former Black Basta affiliates enabled its rise to the #1 position, while new entrants like CipherForce and TeamPCP introduced novel attack patterns combining supply chain compromise with traditional encryption-based extortion. March 2026’s 832 victims represents the highest single-month count observed by HACKURITY in Q1 tracking.

3. Monthly Trend Analysis

Q1 2026 exhibited a clear upward trajectory in ransomware activity, with each successive month recording higher victim counts than the last. This pattern reflects both seasonal factors (organizations returning from end-of-year freezes with unpatched systems) and structural shifts in the ransomware ecosystem.

Month	Victims	% of Q1	Key Events
January 2026	702	30.3%	Post-holiday exploitation surge; Fortinet CVE-2024-55591 mass scanning
February 2026	784	33.8%	Black Basta chat leak; affiliate redistribution begins
March 2026	832	35.9%	ShinyHunters EU campaign; TeamPCP/CipherForce supply chain blitz
Q1 Total	2,318	100%	+18.5% growth January to March

Trend Analysis

The 18.5% increase from January to March follows a pattern consistent with ransomware ecosystem dynamics: the Black Basta dissolution in February created a temporary supply of experienced operators seeking new affiliations. By March, these operators had integrated into Qilin, TheGentlemen, and newly formed groups like CipherForce, resulting in the highest monthly victim count of the quarter. If this trajectory holds, Q2 2026 is projected to exceed 2,500 victims.

4. Most Active Ransomware Groups

The table below presents the 15 most prolific ransomware and data extortion groups observed during Q1 2026, ranked by confirmed victim count. Victim attribution is based on data leak site postings tracked by HACKURITY’s continuous monitoring infrastructure, cross-referenced with ransomware.live community intelligence feeds.

Rank	Group	Victims	% Share	Primary Targets
1	Qilin	370	16%	US, FR, CA, GB, DE
2	TheGentlemen	186	8%	US, DE, IT, FR, GB
3	Akira	185	8%	US, CA, GB, DE, AU
4	IncRansom	145	6.3%	US, GB, CA, IN, BR
5	Nightspire	132	5.7%	US, DE, FR, GB, IT
6	Clop	127	5.5%	US, GB, DE, CA, NL
7	Play	123	5.3%	US, CA, DE, GB, BR
8	DragonForce	113	4.9%	US, GB, CA, AU, IN
9	LockBit5	92	4%	US, IT, FR, DE, ES
10	Sinobi	81	3.5%	JP, US, KR, TW, DE
11	SafePay	78	3.4%	US, CA, GB, DE, AU
12	Medusa	74	3.2%	US, IN, GB, BR, DE
13	ShinyHunters	68	2.9%	EU, US, FR, DE, GB
14	FunkSec	65	2.8%	US, IL, IN, BR, GB
15	RansomHub	62	2.7%	US, GB, CA, DE, FR

Group Ecosystem Analysis

Qilin’s dominance (370 victims, 16% market share) reflects a consolidation trend in the ransomware ecosystem. The group’s sophisticated RaaS platform, combined with the influx of former Black Basta affiliates, has created a highly efficient operation targeting across all major sectors. TheGentlemen and Akira maintain competitive pressure, while newcomers like Nightspire and Sinobi demonstrate the continued low barrier to entry for ransomware operations. LockBit5’s presence (92 victims) confirms the brand’s resilience despite sustained law enforcement pressure throughout 2024-2025.

5. Sector Analysis

Ransomware groups continue to target sectors with high operational disruption potential and perceived willingness to pay. Technology and Manufacturing remain the most impacted verticals, while Healthcare's persistent targeting raises significant public safety concerns.

Rank	Sector	Victims	% Share	Risk Assessment
1	Technology	268	11.6%	CRITICAL
2	Manufacturing	255	11%	CRITICAL
3	Healthcare	152	6.6%	CRITICAL
4	Construction	114	4.9%	HIGH
5	Financial Services	113	4.9%	HIGH
6	Business Services	102	4.4%	HIGH
7	Transportation & Logistics	73	3.1%	MEDIUM
8	Education	72	3.1%	MEDIUM
9	Consumer Services	69	3%	MEDIUM
10	Public Sector	68	2.9%	MEDIUM
11	Legal	55	2.4%	MEDIUM
12	Energy & Utilities	48	2.1%	ELEVATED
13	Real Estate	44	1.9%	ELEVATED
14	Food & Agriculture	38	1.6%	ELEVATED
15	Retail	35	1.5%	ELEVATED

Sector Intelligence

- > **Technology sector** (268 victims) continues to lead, driven by the high value of intellectual property and the sector's expansive attack surface from cloud services and SaaS platforms
- > **Manufacturing** (255 victims) faces dual pressure from traditional ransomware encryption disrupting OT systems and data extortion targeting proprietary design documents
- > **Healthcare** (152 victims) remains critically vulnerable; patient data commands premium dark web pricing and operational disruption creates immediate life-safety urgency to pay
- > **Public Sector** (68 victims) targeting reflects continued interest in government data and critical infrastructure disruption

6. Geographic Impact

The geographic distribution of ransomware victims continues to reflect economic targeting: nations with large GDP, high digitalization, and significant insurance coverage concentrations dominate the victim landscape. The United States alone accounts for over 41% of all Q1 2026 victims.

Rank	Code	Country	Victims	% Share
1	US	United States	957	41.3%
2	DE	Germany	89	3.8%
3	CA	Canada	76	3.3%
4	GB	United Kingdom	75	3.2%
5	FR	France	63	2.7%
6	IT	Italy	63	2.7%
7	IN	India	43	1.9%
8	ES	Spain	40	1.7%
9	BR	Brazil	40	1.7%
10	JP	Japan	31	1.3%
11	AU	Australia	29	1.3%
12	NL	Netherlands	24	1%
13	IL	Israel	22	0.9%
14	KR	South Korea	19	0.8%
15	MX	Mexico	18	0.8%
16	BE	Belgium	16	0.7%
17	CH	Switzerland	15	0.6%
18	PT	Portugal	14	0.6%
19	SE	Sweden	13	0.6%
20	AT	Austria	12	0.5%

European Targeting Escalation

European nations collectively account for a significant share of Q1 victims: Germany (89), United Kingdom (75), France (63), Italy (63), Spain (40), Netherlands (24), Belgium (16), Switzerland (15), Portugal (14), Sweden (13), and Austria (12)—totaling **424 European victims** or **18.3%** of all Q1 activity. The ShinyHunters campaign specifically targeting EU institutions and the CipherForce automotive sector blitz demonstrate deliberate strategic interest in European critical infrastructure.

7. Initial Access Vectors & Exploited CVEs

HACKURITY's honeypot sensor network provides direct visibility into the CVEs being actively exploited by ransomware affiliates for initial access. The following vulnerabilities were observed in active exploitation during Q1 2026, with confirmed links to ransomware group operations.

CVE / Product	Description	Severity	Linked Groups
CVE-2024-55591 Fortinet FortiOS	Authentication bypass via crafted Node.js websocket requests allows remote attackers to gain super-admin privileges	CRITICAL (9.8)	SuperBlack, Mora_001 Active since January 2025
CVE-2025-22457 Ivanti Connect Secure	Stack-based buffer overflow in Ivanti Connect Secure, Policy Secure, and ZTA Gateways allows unauthenticated RCE	CRITICAL (9.0)	UNC5221 (China-nexus) Active since March 2025
CVE-2025-24472 Fortinet FortiOS	CSF proxy request authentication bypass enabling unauthorized super-admin access to FortiGate appliances	CRITICAL (8.1)	SuperBlack Active since February 2025
CVE-2023-6549 Citrix NetScaler ADC/Gateway	Unauthenticated buffer overflow in AAA virtual server allowing denial-of-service and potential RCE	HIGH (8.2)	Multiple RW affiliates Active since January 2024
CVE-2023-4966 Citrix NetScaler ADC/Gateway	Session token disclosure (CitrixBleed) enabling authenticated session hijack without credentials	CRITICAL (9.4)	LockBit, ALPHV/BlackCat affiliates Active since October 2023

HACKURITY Sensor Intelligence

These CVEs are not theoretical—HACKURITY's globally distributed honeypot sensors recorded sustained exploitation attempts against all five vulnerabilities throughout Q1 2026. CVE-2024-55591 (Fortinet authentication bypass) and CVE-2025-22457 (Ivanti buffer overflow) exhibited the highest daily attempt volumes, consistent with automated scanning by ransomware affiliate botnets. Organizations running unpatched Fortinet, Ivanti, or Citrix edge appliances should assume active targeting and prioritize emergency patching.

8. Notable Q1 2026 Campaigns

Four major ransomware and data extortion campaigns defined the Q1 2026 threat landscape. Each represents a distinct operational model and strategic shift in the ransomware ecosystem. HACKURITY produced dedicated Threat Intelligence Bulletins for all four campaigns.

Black Basta Internal Leak & Operational Dissolution

February 2026

A massive trove of internal Black Basta chat logs was publicly leaked in February 2026, exposing the group's operational playbooks, affiliate management structures, ransom negotiation scripts, and internal conflicts. The leak revealed connections between Black Basta operators and the former Conti ransomware syndicate, including shared infrastructure and money laundering channels. Following the leak, Black Basta operations effectively ceased, with key operators fragmenting into splinter cells including CipherForce and elements absorbed by Qilin and TheGentlemen. HACKURITY published TB-2026-0217-001 documenting the full threat actor profile and operational impact.

ShinyHunters European Cloud Breach Campaign

March 2026

ShinyHunters (operating as SLH) conducted an aggressive data extortion campaign targeting major European enterprises and institutions throughout March 2026. Confirmed victims included a major European automotive manufacturer, a European rail transport company SA, a leading European aerospace manufacturer SE, and a US technology company, with the crown jewel being a 344GB exfiltration from a major EU government institution AWS cloud infrastructure. The campaign exploited misconfigured S3 buckets, stolen CI/CD tokens, and supply chain access vectors. HACKURITY produced five threat bulletins (TB-2026-0319-001 through TB-2026-0328-001) tracking the full campaign evolution, including TLP:RED advisories for affected customers.

TeamPCP Multi-Ecosystem Supply Chain Attack

March 2026

TeamPCP emerged as a new threat actor executing a sophisticated multi-ecosystem supply chain campaign. Starting from a stolen GitHub personal access token, the group pivoted through npm, PyPI, and Docker Hub ecosystems, injecting malicious dependencies into widely-used packages. The campaign culminated in a ransomware alliance with CipherForce, which exploited IDOR vulnerabilities to breach a major European automotive manufacturer and 36+ automotive manufacturers. HACKURITY published TB-2026-0326-001 (supply chain analysis) and TB-2026-0326-003 (CipherForce automotive sector flash alert), with customer-specific advisories under TB-2026-0326-002.

CipherForce Automotive Sector Blitz

March 2026

CipherForce, a splinter group emerging from dissolved Black Basta operators, partnered with TeamPCP to execute a targeted blitz against the automotive sector. Leveraging IDOR vulnerabilities in supplier portal APIs, CipherForce exfiltrated design documents, production schedules, and employee PII from a major European automotive manufacturer and cascaded access to 36+ connected OEMs and Tier-1 suppliers. The attack demonstrated the lethal combination of supply chain compromise (TeamPCP) with traditional ransomware extortion (CipherForce). HACKURITY issued a flash alert (TB-2026-0326-003) warning of active data exfiltration in progress.

9. HACKURITY Threat Bulletins Issued

HACKURITY Threat Intelligence produced 10 dedicated threat bulletins during Q1 2026, providing customers with actionable intelligence on emerging campaigns, threat actor profiles, and exposure analyses. The following table summarizes all bulletins issued during the reporting period.

Bulletin ID	Title	Date
TB-2026-0217-001	Black Basta Ransomware Group - Threat Actor Profile	2026-02-17
TB-2026-0225-001	Aviation Sector - DevOps Environment Exposure	2026-02-25
TB-2026-0319-001	Automotive Sector - ShinyHunters/SLH Exposure	2026-03-19
TB-2026-0319-002	Rail/Transport Sector - ShinyHunters/SLH Exposure	2026-03-19
TB-2026-0319-003	Aviation Sector - ShinyHunters Campaign Extension	2026-03-19
TB-2026-0319-004	Technology Sector - ShinyHunters Exposure	2026-03-19
TB-2026-0326-001	TeamPCP Supply Chain Campaign	2026-03-26
TB-2026-0326-002	TeamPCP Customer Threat Advisory	2026-03-26
TB-2026-0326-003	Automotive Sector - CipherForce Active Breach Flash Alert	2026-03-26
TB-2026-0328-001	EU Government Institution - ShinyHunters Cloud Breach (350GB)	2026-03-28

Intelligence Production Summary

- > **10 bulletins** issued across Q1 2026, covering 4 distinct campaigns and multiple affected organizations across sectors
- > **3 customer-specific advisories** delivered under restricted classifications
- > **1 flash alert** issued for active breach (CipherForce targeting automotive sector) with immediate customer notification via Slack
- > Average time from event detection to bulletin publication: < **24 hours** for flash alerts, < **72 hours** for full analysis bulletins

10. Strategic Outlook & Recommendations

Q2 2026 Threat Projections

Projection 1

Qilin is projected to maintain dominance, with estimated 400+ victims in Q2 based on current trajectory and absorption of former Black Basta affiliates

Projection 2

Supply chain attacks will intensify as TeamPCP-style campaigns prove operationally efficient; expect similar CI/CD token theft campaigns targeting European critical infrastructure

Projection 3

LockBit5 rebrand activity will likely escalate as the group attempts to regain market share lost during 2025 law enforcement disruptions

Projection 4

Cloud-native attacks (S3 bucket exploitation, IAM role abuse) will surpass traditional VPN exploitation as the primary initial access vector for data extortion groups

Projection 5

The automotive and manufacturing sectors face elevated risk from CipherForce and similar groups targeting OEM supply chain interconnections

HACKURITY Recommendations

Defensive Priorities for Q2 2026

1. Implement strict SCM token rotation policies (max 24h lifetime) and audit all CI/CD pipeline dependencies for supply chain integrity
2. Deploy cloud security posture management (CSPM) with automated S3 bucket policy enforcement to prevent ShinyHunters-style cloud breaches

3. Prioritize patching of CVE-2024-55591 and CVE-2025-22457 on all Fortinet and Ivanti edge appliances; these remain actively exploited initial access vectors
4. Conduct API security assessments focusing on IDOR vulnerabilities in supplier portals and B2B integration endpoints
5. Subscribe to HACKURITY Threat Intelligence for real-time alerts on emerging ransomware campaigns and targeted threat bulletins



HACKURITY Security Operations

For inquiries regarding this report or to subscribe to HACKURITY Threat Intelligence, contact security@hackurity.io or reach us on [#tech Slack](#).

Data sources: ransomware.live, HACKURITY honeypot sensor network, HACKURITY threat bulletin archive.
Report generated: April 1, 2026

Made with ♥ by Hekuriti Szekuriti