ThreatCluster

Q1 2026 Threat Intelligence Report



Published: March 2026
Author: Epsilon Research, ThreatCluster
Classification: TLP:WHITE

threatcluster.io
hello@threatcluster.io

Contents

- Executive Summary
- The Dataset
  - What the Numbers Mean
  - Monthly Volume
  - Source Diversity
  - Entity Extraction
  - From Collection to Analysis: What This Means for an Analyst
- The Iran Escalation
- APT Landscape
  - Chinese APT Proliferation
  - Russian Operations
  - North Korea: Unexplained Quiet
  - Declining and Disappeared
- The Ransomware Shake-Up
  - Established Groups Collapsing
  - Fragmentation: The Defining Characteristic
  - Law Enforcement Impact
- The Cisco Zero-Day Pattern
- The Zero-Day Economy
  - Critical Zero-Days
  - Notable Zero-Day Clusters
- Supply Chain Acceleration
- The Poland Energy Grid Attack
- Malware Trends
  - New Malware Families
  - AI-Themed Malware
  - Infostealer Market Churn
  - Disappeared Malware

Contents

- AI as Attack Surface
  - AI as Tool
  - AI as Target
  - AI Agents
- Platform Targeting
- Industry and Geopolitical Targeting
  - Nation-State Cluster Attribution
- MITRE ATT&CK and Attack Vector Analysis
- Campaigns
- IOCs and Technical Indicators
- Law Enforcement Operations
- Outlook: Q2 2026
- Methodology

Executive Summary

ThreatCluster processed 53,062 articles from 6,753 unique sources across Q1 2026, reducing them to 6,092 actionable threat intelligence clusters through density-based semantic clustering, an 89% noise reduction rate.

The platform extracted 11,668 unique entities and tracked 3,060 new CVEs, 511 new malware families, 230 new APT groups, and 88 new ransomware groups, all first seen in Q1. Only 35 clusters (0.6%) scored Critical or High (80+). Every one of those mapped to a confirmed high-impact incident.

Three dynamics define the quarter.

Iran became the dominant nation-state threat.

Mentions increased 6.7x (121 to 808) quarter-over-quarter. The US-Israeli strikes on 28 February triggered the most significant cyber-kinetic convergence since the Russia-Ukraine conflict. Handala, an MOIS-affiliated proxy group, went from zero mentions to 35 in March alone, escalating from claimed healthcare breaches to the Stryker medical device wiper attack (262 articles) and the breach of FBI Director Kash Patel's personal email within a single month.

The energy sector saw a 113% increase in targeting. March's average threat score spiked to 52.0, a 51% increase over January and February, meaning the baseline severity of reported threats rose across the board. Lower-severity activity did not disappear. It was drowned out.

threatcluster.io
hello@threatcluster.io
71-75 Shelton Street, Covent Garden, London, WC2H 9JQ

The ransomware landscape fragmented.

Clop collapsed 79%. Akira dropped 69%. BlackCat/ALPHV fell to near-extinction. 88 new ransomware groups appeared in Q1, roughly one new group per day. The established hierarchy is dissolving into a distributed ecosystem of smaller operators with shorter operational lifespans. Interlock's 467% growth in March, driven entirely by Cisco zero-day exploitation, is the model for this new approach: build an operation around a specific vulnerability rather than maintaining broad access capabilities. Meanwhile, groups are vanishing as fast as they appear. Gentlemen, Makop, VolkLocker, Nefilim, Blackbyte, and HelloKitty all disappeared in Q1. The churn rate is now the defining characteristic of the ransomware ecosystem



Surveillance and security infrastructure became the primary target.

Chinese APTs compromised FBI wiretap systems, all four Singaporean telcos, and lawful intercept infrastructure at nine US telecommunications providers. Russian state actors hijacked government officials' Signal and WhatsApp accounts. The Coruna iOS exploit kit leaked from a commercial surveillance vendor to Russian espionage to Chinese cybercrime in under twelve months, using exploit techniques linked to Operation Triangulation. The systems built to provide security are the attack surface.

The Dataset

ThreatCluster aggregates open-source threat intelligence through density-based semantic clustering (DBSCAN). Articles are collected from RSS feeds, vendor advisories, government alerts, security blogs, news outlets, social media, and dark web sources. Related articles are grouped by meaning rather than keyword, and structured entities are extracted automatically.

threatcluster.io
hello@threatcluster.io
71-75 Shelton Street, Covent Garden, London, WC2H 9JQ

Metric	Q1 2026	Q4 2025	Change
Articles processed	53,062	30,430	+74%
Clusters identified	6,092	4,858	+25%
Unique sources	6,753	4,204	+61%
Articles per day	603	422	+43%
Clustering ratio	8.7:1	6.3:1	Improved
Noise reduction	~89%	~84%	Improved

What the numbers mean

The clustering ratio of 8.7:1 means that for every cluster ThreatCluster generates, an average of 8.7 source articles are grouped together. An analyst checking those sources manually would read 8.7 articles to get the same intelligence that one cluster provides.

At 603 articles per day, that is over 17 hours of manual reading reduced to approximately 69 actionable clusters. The ratio improved from 6.3:1 in Q4 2025, meaning the platform gets better at deduplication as it scales. More input, proportionally less output, higher quality per cluster.

threatcluster.io
hello@threatcluster.io
71-75 Shelton Street, Covent Garden, London, WC2H 9JQ

The scoring system concentrated signal effectively. Only 35 clusters (0.6%) scored Critical or High. Each of those 35 clusters mapped to a genuine high-impact incident: Apple zero-day, Cisco zero-day campaign, APT28 MSHTML exploitation, Poland energy grid attack. The platform is not inflating severity. It is compressing 53,062 articles into the 35 that demand immediate attention and the 460 (Medium-High) that require monitoring.

Monthly volume

Month	Articles	Clusters	Avg Score	Max Score
January	15,111	1,991	34.2	95.89
February	18,683	2,071	34.5	96.31
March	19,268	2,030	52.0	94.31

March's average threat score spiked to 52.0. That is a 51% increase over the January/February baseline. The spike was driven by the Iran-US military escalation and associated cyber operations, but the effect is structural: when the average cluster scores 52 instead of 34, the noise floor rises. Analysts relying on manual triage lose visibility on lower-tier activity because the high-severity volume demands all available attention.

Source diversity

The top source (Microsoft MSRC at 2,054 articles) accounts for only 3.9% of total volume. No single source dominates. The long tail is where value surfaces: stories like DynoWiper (13 mentions), RustyWater (7), and UAT-7290 (5) emerged from smaller specialist sources that would not appear in a typical RSS feed setup.

The fact that Microsoft's own security advisories generate the most articles reinforces how much of "threat intelligence" is functionally patch management. ThreatCluster separates the two by clustering vulnerability disclosures away from actor-driven threat intelligence.

Rank	Source	Articles
1	Microsoft MSRC	2,054
2	LinuxSecurity	1,762
3	CybersecurityNews	1,351
4	Hacker News (YC)	1,167
5	The Register	1,116
6	GBHackers	1,014
7	YouTube	814

Rank	Source	Articles
8	SC World	767
9	TechCrunch	634
10	BleepingComputer	619

Entity extraction

11,668 unique entities across 17 entity types, generating over 56,000 mentions in Q1. 3,060 new CVEs first seen in Q1. 511 new malware families. 230 new APT groups. 88 new ransomware groups. 1,618 new companies. 624 new tools.

That is the pace at which the threat landscape is expanding. One platform tracking all of it. The "new in Q1" column is as important as the totals. Knowing that a malware family or APT group was first observed this quarter rather than last year changes how an analyst prioritises it.

Entity type	Unique	Mentions	New in Q1
Attack types	78	10,509	37
Countries	211	7,957	57
Platforms	2,164	7,831	1,638
CVEs	3,306	7,361	3,060

Entity type	Unique	Mentions	New in Q1
Companies	2,020	6,734	1,618
MITRE ATT&CK	229	4,811	127
Industries	105	2,508	54
Tools	818	2,459	624
Malware	666	1,989	511
APT groups	321	1,196	230
Domains (IOC)	605	826	544
Campaigns	399	739	368
Ransomware groups	145	564	88
Vulnerabilities	291	538	247
IOC hashes (all)	255	279	152
IPv4	46	61	44
Crypto addresses (all)	9	10	9

What this means for an analyst

The volume problem in threat intelligence is not a lack of information. It is too much of it. 603 articles per day from 6,753 sources. No analyst can read that. **At a conservative 2 minutes per article (skim, assess relevance, extract key details, decide whether to act), that is 1,206 minutes per day. Over 20 hours. It is physically impossible for one person.**

ThreatCluster reduces that load in four compounding layers.

1

Layer 1: Clustering

The 8.7:1 ratio reduces 603 daily articles to approximately 69 clusters. When a Cisco zero-day drops, 11 articles appear across The Register, BleepingComputer, CybersecurityNews, SC World, vendor blogs, Reddit, and LinkedIn.

An analyst checking sources manually reads all 11 before realising it is the same story. Then they mentally correlate which details each source adds. Then they write it up.

ThreatCluster clusters those 11 articles into one group, extracts the CVE, the affected product, the threat actor (if attributed), the MITRE ATT&CK technique, and the severity. The analyst reads one cluster, rathen than 10 individual articles.

threatcluster.io
hello@threatcluster.io
71-75 Shelton Street, Covent Garden, London, WC2H 9JQ

2

Layer 2: Personalised filtering

The ~69 daily clusters represent the unfiltered global feed. Every sector, every country, every actor. A SOC analyst at a UK energy company does not need 90% of that. They need energy sector targeting, OT/ICS threats, CVEs affecting their Cisco/Fortinet/Schneider stack, and the threat actors known to target their industry.

Custom keyword and entity tracking filters those 69 clusters down to the 5-10 directly relevant to the analyst's organisation. ThreatCluster supports over 30,000 trackable entities plus custom keywords.

The daily digest at 6am UTC contains only what matches the analyst's configuration. The daily review drops from 4-6 hours (69 clusters) to 15-30 minutes (5-10 relevant clusters).

3

Layer 3: Alerting

Of those 5-10 relevant clusters, 1-2 may hit a threshold that triggers an immediate alert: a score above 80, a specific CVE matching the analyst's stack, a named threat actor entering their sector. Those alerts arrive in real time rather than waiting for the morning digest. The "are we affected?" answer arrives before leadership asks the question.

threatcluster.io
hello@threatcluster.io
71-75 Shelton Street, Covent Garden, London, WC2H 9JQ

4

Layer 4: Reporting

The analyst selects the relevant clusters from the week, chooses a report style (executive, technical, threat advisory, incident response, compliance, or custom), and generates a report. The weekly threat brief that previously required a full day of manual collation, cross-referencing, and writing now takes under an hour. The entities are already extracted. The sources are already deduplicated. The structure is already there.

Each layer compounds...

Stage	Daily volume (avg)	Time required
Raw articles	603	~20 hours (impossible)
After clustering	69 clusters	4-6 hours
After personalised filtering	5-10 clusters	15-30 minutes
After alerting	1-2 critical alerts	Real-time, minutes
Weekly reporting	Selected clusters	Under 1 hour

threatcluster.io
hello@threatcluster.io
71-75 Shelton Street, Covent Garden, London, WC2H 9JQ

The shift is not just about time. It changes what the analyst does with their day. Without clustering, the job is collection: trawling feeds, reading articles, deduplicating mentally, copying data into spreadsheets. That is labour, not analysis. With clustering, the analyst starts the day with pre-structured intelligence groups, each with extracted entities and severity scores. The work becomes triage, assessment, and response rather than collection.

The Iran escalation

Iran is the story of Q1 2026. No other shift in the data comes close.

Metric	Q4 2025	Q1 2026	Change
Iran mentions	121	808	+568% (6.7x)
Israel mentions	45	356	+691%
Iran-attributed clusters	33	225	Avg score 57.1

The crisis traces to December 2025 protests in Tehran, escalated through failed nuclear talks in February, and culminated in Operation Epic Fury (US) and Operation Roaring Lion (Israel) on 28 February.

US Cyber Command confirmed operating as "first movers" in the operation, layering non-kinetic effects to disrupt Iranian communications and sensor networks. Operation Epic Fury generated 37 mentions across the quarter, the most referenced named campaign.

Handala emerged as the quarter's breakout threat actor (0 mentions in January and February, 35 in March). Assessed by Palo Alto Networks as a persona of Void Manticore (MOIS-affiliated), the group's trajectory within a single month was steep.

The Stryker medical device wiper attack on 11 March (262 articles, the fourth most-covered story of the quarter) saw Handala gain access to Stryker's Microsoft Intune console and issue remote wipe commands across the entire estate, affecting operations in 79 countries. The group claimed to have wiped over 200,000 systems and exfiltrated 50 terabytes of data.

Later in March, Handala claimed FBI Director Kash Patel's personal email, with the DOJ confirming the breach and TechCrunch verifying leaked emails using cryptographic signatures.

ThreatCluster tracked Handala from its first mention. For an analyst relying on manual collection, the group's activity would have surfaced days or weeks after the platform had already clustered it.

Iran's broader cyber response to the US strikes generated 394 articles (the second most-covered story).

The Electronic Operations Room, established on 28 February, coordinated approximately 60 hacktivist groups. MuddyWater deployed the RustyWater RAT (a Rust-based implant targeting Israeli government, military, and financial organisations).



The Dust Specter campaign targeted Iraqi Ministry of Foreign Affairs officials with four previously undocumented malware families. CloudSEK documented a trojanised Red Alert rocket warning app distributed via SMS spoofing during active missile strikes.

Gulf state mentions surged across the board: Qatar (5 to 76), Kuwait (6 to 57), Bahrain (0 to 50), UAE (18 to 72), Saudi Arabia (23 to 89). Every one of these increases correlates directly with the conflict's expansion into Gulf territory.

Gulf state mentions surged across the board: Qatar (5 to 76), Kuwait (6 to 57), Bahrain (0 to 50), UAE (18 to 72), Saudi Arabia (23 to 89). Every one of these increases correlates directly with the conflict's expansion into Gulf territory.

The wiper malware DynoWiper appeared for the first time in Q1 (13 mentions), consistent with Iranian destructive playbooks previously seen with ZeroCleare, Dustman, Shamoon, and Meteor.

Key clusters

Iran's Cyber Response to U.S. Military Strikes Expected Amid Rising Tensions
394 articles / 244 sources

https://threatcluster.io/cluster/b09a5102

Iran-Linked Handala Group Launches Cyberattack on Stryker Medical Technology
262 articles / 190 sources

https://threatcluster.io/cluster/f39b53be

Trump Threatens to Obliterate Iran's Power Plants Amid Escalating Conflict
123 articles / 53 sources

https://threatcluster.io/cluster/bf20deb1

State Actors Utilize AI for Misinformation in Iran War
8 articles / 8 sources

https://threatcluster.io/cluster/155243f6

The APT Landscape

Rank	Group	Q1 mentions	Monthly trend (J/F/M)	Attribution
1	Salt Typhoon	75	22 / 31 / 22	China (MSS)
2	APT28	51	4 / 30 / 17	Russia (GRU)
3	UNC3886	48	3 / 41 / 4	China
4	Handala	35	0 / 0 / 35	Iran (MOIS)
5	Lazarus Group	33	11 / 18 / 4	North Korea
6	ShinyHunters	33	11 / 15 / 7	Cybercrime
7	Volt Typhoon	28	9 / 5 / 14	China
8	Kimsuky	26	19 / 4 / 3	North Korea
9	Konni	24	17 / 2 / 5	North Korea
10	Sandworm	24	11 / 10 / 3	Russia (GRU)

Chinese APT proliferation

China dominated the APT landscape in Q1, with 147 attributed clusters at an average score of 47.0. Three dynamics stand out.



UNC3886 was the biggest new APT entrant of the quarter, going from zero mentions in Q4 to 48 in Q1.

The group's activity concentrated almost entirely in February (41 of 48 mentions), driven by Singapore's disclosure of Operation Cyber Guardian (20 mentions), an 11-month operation involving over 100 personnel to evict UNC3886 from all four major Singaporean telcos (Singtel, StarHub, M1, Simba Telecom).

The group uses zero-day exploits against perimeter firewalls, installs rootkits for persistence, and targets the infrastructure layer of networks rather than endpoints.

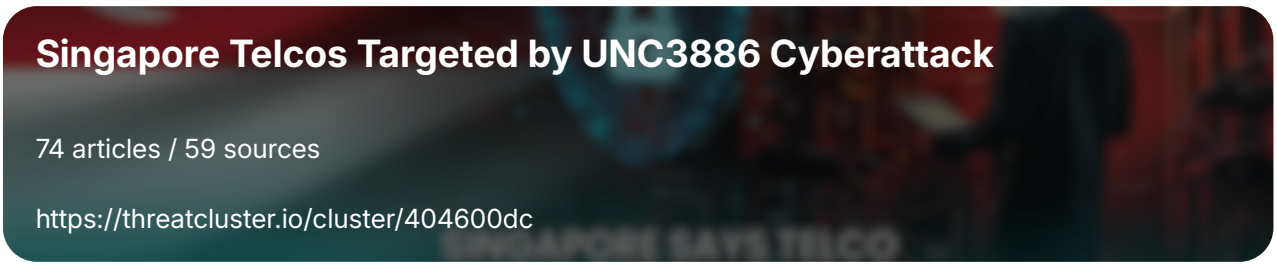
ThreatCluster tracked UNC3886 from its first mention in January, well before the group entered mainstream reporting in February.

Salt Typhoon maintained the top position at 75 mentions (up from 45 in Q4), sustaining consistent activity across all three months. The group's campaign against US telecommunications providers extended into Q1 with the FBI wiretap system breach disclosed in March. Salt Typhoon has now compromised lawful intercept systems at nine US telcos and breached over 200 companies across 80 countries.

Volt Typhoon resurged in March (14 mentions, up from 5 in February), continuing its focus on US critical infrastructure pre-positioning. The group's sustained activity alongside Salt Typhoon and UNC3886 represents three parallel Chinese campaigns targeting telecommunications, critical infrastructure, and network edge devices respectively.

New Chinese-nexus groups first tracked in Q1 include UNC2814 (12 mentions), UNC6201 (11), Lotus Blossom (11), Gallium (9), and UAT-7290 (5, telecom espionage).

Key clusters





Russian operations

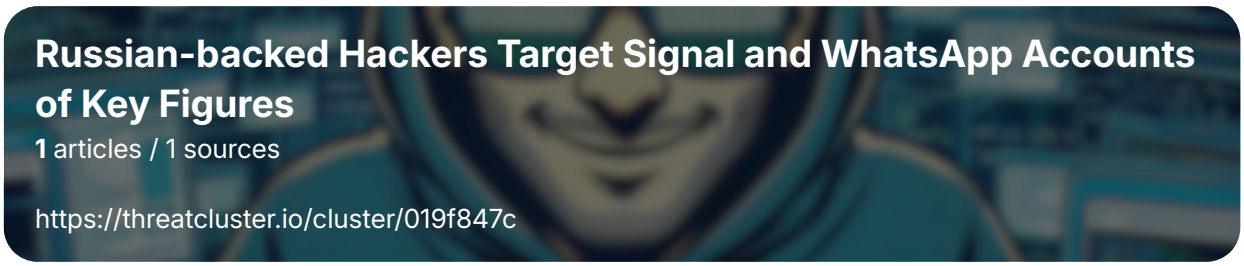
APT28 (Fancy Bear) spiked to 51 mentions, with 30 in February alone driven by exploitation of an MSHTML zero-day (CVE-2026-21509, score 94.31). The Dutch MIVD/AIVD disclosed a Russian campaign hijacking Signal and WhatsApp accounts of government officials, military personnel, and civil servants on 9 March (126 articles). The attackers impersonate Signal's support team, persuade targets to share verification codes, and register new devices to access contacts and group chats. The attack bypasses end-to-end encryption entirely by compromising the account itself.



Sandworm declined (11 to 10 to 3) across the quarter, as did several Russian-linked groups. The shift may reflect operational reallocation toward the Iran conflict theatre or improved operational security reducing open-source visibility.

Key clusters





North Korean operations

North Korean activity declined across all tracked groups in Q1. This is unusual and warrants attention.

Group	January	February	March	Trend
Lazarus Group	11	18	4	Declining
Kimsuky	19	4	3	-84%
Konni	17	2	5	-71%
APT38	0	0	0	Disappeared (was 16 in Q4)

57 total DPRK-attributed clusters, average score 45.7. Lazarus peaked in February (18) then dropped to 4 in March. Kimsuky collapsed from 19 to 3. Konni from 17 to 5. APT38 disappeared entirely (16 mentions in Q4, zero in Q1).



North Korean groups have historically maintained steady operational tempos regardless of geopolitical events. The collective decline across all DPRK-linked groups in a single quarter is anomalous.

Possible explanations include improved operational security reducing open-source footprint, operational reallocation, internal disruption, or simply a gap between campaigns.

The data does not explain the cause. It does identify the pattern.

threatcluster.io
hello@threatcluster.io
71-75 Shelton Street, Covent Garden, London, WC2H 9JQ

Declining and disappeared

Several APT groups that were active in Q4 2025 declined sharply or vanished:

- Scattered Spider: 27 to 11 (largest drop of an active group)
- APT38: 16 to 0 (disappeared)
- Stealth Falcon: 11 to 0 (disappeared)
- ArcaneDoor: 10 to 0 (disappeared)
- PlushDaemon: 10 to 0 (disappeared)
- Gamaredon: 8 to 0 (disappeared)

The disappearance data is intelligence in itself. Tracking what vanished is as valuable as tracking what appeared. Most platforms only surface what is trending up. A previously active group going silent is an intelligence signal: either they improved OPSEC, shifted to targets that do not generate public reporting, or they are being disrupted. ThreatCluster surfaces both directions.



The Ransomware Shake-up

The ransomware landscape underwent its most significant structural change since the Conti dissolution in 2022.

Group	Q4 2025	Q1 2026	Change
Clop (combined)	109	23	-79%
Akira	70	22	-69%
BlackCat/ALPHV	62	8	-87%
LockBit	43	30	-30%
DragonForce	21	11	-48%
RansomHouse	15	2	-87%

Clop's collapse is the headline number. From 109 combined mentions in Q4 to 23 in Q1, a 79% drop. The group's mass exploitation campaigns (MOVEit, GoAnywhere) defined 2023-2024. Q1 2026 data suggests the model has run its course, whether through law enforcement pressure, reduced access to new mass-exploitation vectors, or operational choice.

BlackCat/ALPHV dropped from 62 combined mentions to 8, continuing the decline following the FBI's seizure of their infrastructure in late 2024. LockBit declined from 43 to 30. The February 2024 law enforcement disruption had lasting impact but did not kill the brand: LockBit5 (2 mentions) appeared in Q1, suggesting a possible rebrand attempt.

Qilin took the nominal top position at 50 mentions but collapsed from February (27) to March (5), suggesting a temporary spike rather than sustained dominance. Everest disappeared entirely in March (13 to 8 to 0). DragonForce vanished (6 to 5 to 0). RansomHub, which was the dominant group in January (15 mentions), collapsed to near-zero (0 in February, 1 in March).

Fragmentation

88 new ransomware groups appeared in Q1 2026. That is roughly one new group per day across 88 days. Compare that number to the groups that disappeared: Gentlemen (6 to 0), Makop (6 to 0), VolkLocker (5 to 0), Nefilim (5 to 0), Blackbyte (5 to 0), HelloKitty (4 to 0).

Groups appear, operate for weeks, and dissolve. The barrier to entry has collapsed. The churn rate is now the defining characteristic of the ransomware ecosystem, not the dominance of any single operator.

Interlock is the model for the new approach. The group went from 2 mentions in Q4 to 23 in Q1, with 17 of those in March alone (467% month-over-month growth). The surge is directly tied to exploitation of Cisco zero-day CVE-2026-20131.

Rather than maintaining broad access capabilities, Interlock built its operation around a single high-value vulnerability in widely deployed enterprise infrastructure.

Expect this model to be replicated.

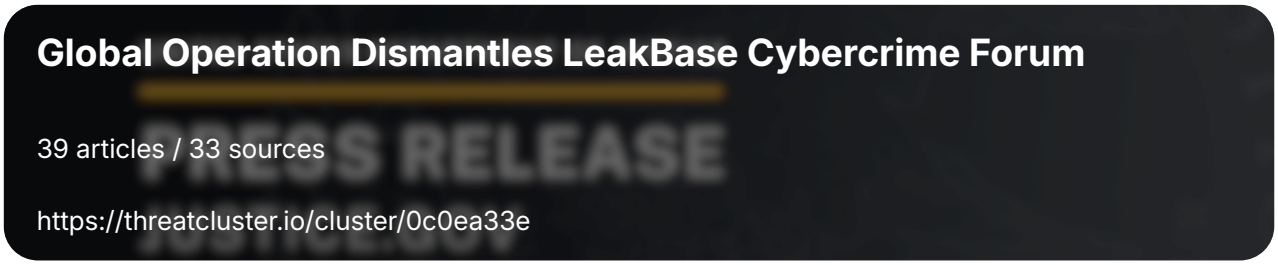
Black Basta resurged from 4 (Q4) to 23 (Q1), though activity was January-heavy (14) and declined through the quarter (5 in February, 4 in March).

AI-themed ransomware entered the ecosystem: PromptLock (6 mentions) and AiLock (4 mentions, new in Q1). Whether these groups use actual AI capabilities or exploit the branding for attention is unclear from open-source reporting.

Notable new entrants: Nova (10), 0apt (10, February-only), Nitrogen (7), LeakNet (6), TridentLocker (5), LockBit5 (2, potential rebrand).

Law enforcement impact

The Phobos ransomware leader pleaded guilty in Q1, facing up to 20 years in prison. Phobos generated 17 mentions across the quarter. The conviction follows the broader pattern of law enforcement action that contributed to BlackCat/ALPHV's collapse and LockBit's sustained decline. Operation Leak (LeakBase seizure) removed a significant credential marketplace that fed the ransomware ecosystem's initial access pipeline.



The Cisco zero-day pattern

Cisco was the single most systematically targeted vendor for zero-day exploitation in Q1 2026. At least four separate zero-day clusters were identified, all scoring above 82.

Cluster	Score	Date	Detail
Cisco AsyncOS Zero-Day	95.80	Jan 16	11 articles
Cisco Federal Networks Zero-Day	92.31	Feb 28	2 articles
Cisco Unified CM Zero-Day	90.96	Jan 22	CVE-2026-20045
Cisco SD-WAN Zero-Day	82.13	Feb 25	104 articles, exploited since 2023

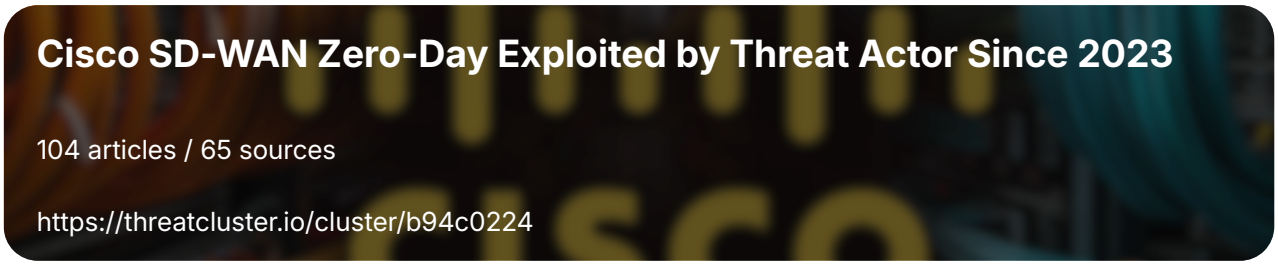
The SD-WAN zero-day is the most concerning. With 104 articles, it was the eighth most-covered story of the quarter. The vulnerability had been exploited since 2023, meaning threat actors had at least three years of access before public disclosure.

Cisco's March patch bundle covered 48 vulnerabilities across Secure Firewall ASA, FMC, and FTD products, including two CVSS 10.0 flaws (CVE-2026-20079 and CVE-2026-20131).

The Interlock ransomware group specifically exploited CVE-2026-20131 for initial access, representing a direct link between zero-day discovery and ransomware monetisation.

This concentration of zero-day activity against a single vendor's product line across multiple product families (AsyncOS, Unified CM, SD-WAN, FMC) indicates either coordinated targeting or systematic vulnerability research focused on Cisco infrastructure.

Organisations running Cisco edge devices should treat this as an active, ongoing campaign rather than a series of unrelated disclosures.



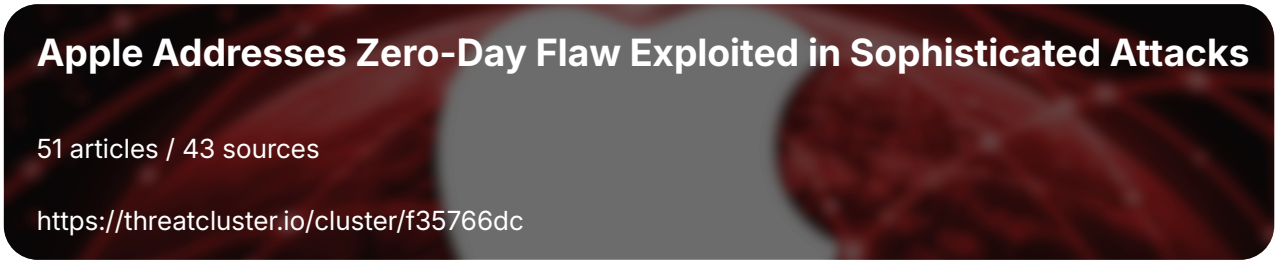
The zero-day economy

Zero-day exploitation more than doubled in Q1 2026.

Metric	Q4 2025	Q1 2026	Change
Zero-day mentions	413	922	+123%

Critical zero-days (score 90+)

Zero-Day	Score	Date
Apple Zero-Day	96.31	Feb 19
CISA Gogs RCE Zero-Day	95.18	Jan 12
Cisco AsyncOS Zero-Day	95.80	Jan 16
APT28 MSHTML Zero-Day	94.31	Mar 2
Microsoft Office CVE-2026-21509	94.31	Jan 27
Cisco Federal Networks Zero-Day	92.31	Feb 28
Chromium CSS Zero-Day	91.29	Feb 22
Cisco Unified CM Zero-Day	90.96	Jan 22



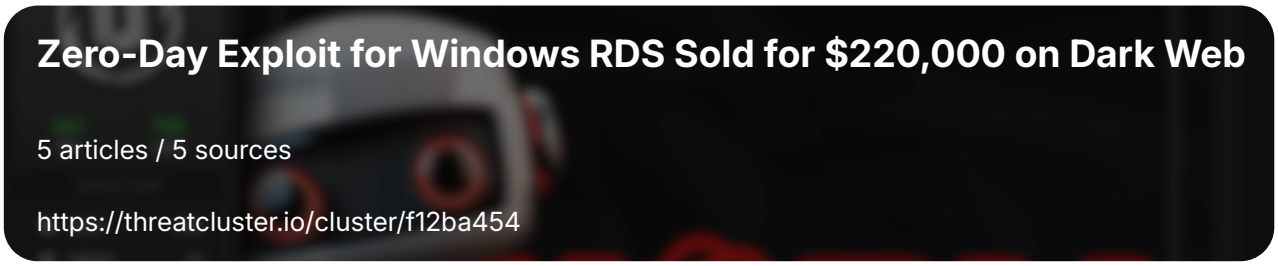
Notable zero-day clusters

The Telegram zero-day (score 76.5) is significant given Telegram's role as the primary coordination platform for hacktivist groups. The Electronic Operations Room, Handala, and all 60+ Iran-aligned hacktivist groups operate through Telegram. A zero-day in that platform's security has direct implications for both attackers' operational security and defenders' ability to monitor hacktivist coordination.

Critical Telegram Zero-Day Vulnerability Exposes User Accounts to Remote Hijacking
3 articles / 3 sources

https://threatcluster.io/cluster/76ff5f88

A Windows RDS zero-day was sold for $220,000 on the dark web (score 71.5), providing a price signal for the underground exploit market and indicating demand for remote access capabilities against enterprise Windows infrastructure

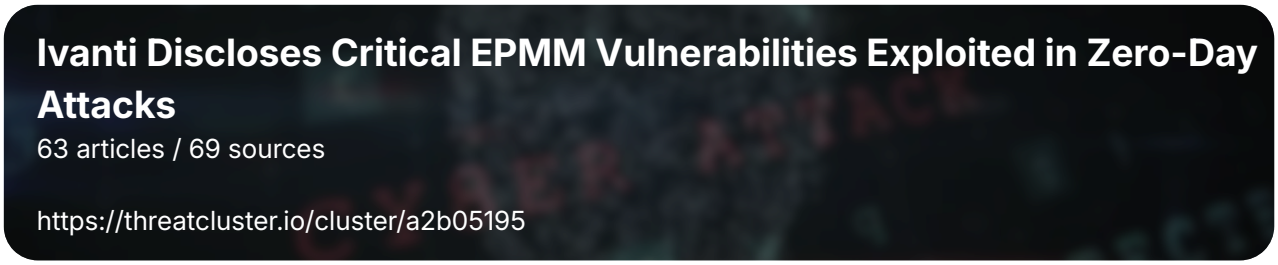


Zero-Day Exploit for Windows RDS Sold for $220,000 on Dark Web

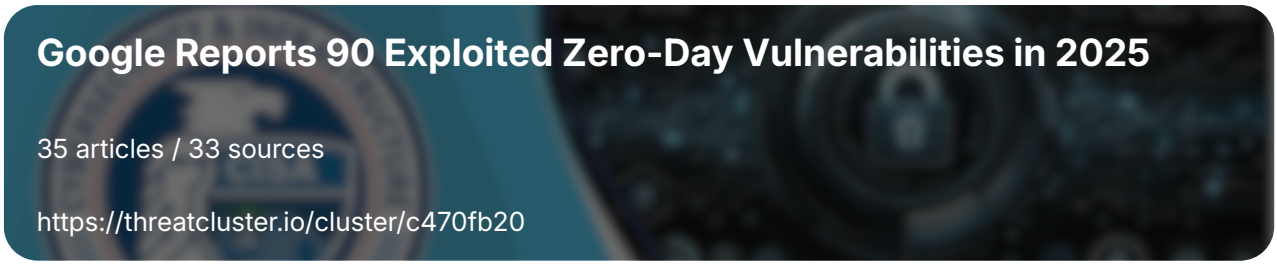
5 articles / 5 sources

https://threatcluster.io/cluster/f12ba454

The Ivanti EPMM zero-day cluster (64 articles, score 74.39) continues the pattern of edge device and mobile device management platforms being targeted. Ivanti has been a recurring target since 2024.



Google's Threat Intelligence Group reported 90 zero-day vulnerabilities exploited in 2025, with commercial surveillance vendors surpassing state-sponsored groups as the top exploiters for the first time. 48% of exploited zero-days targeted enterprise infrastructure. China-linked groups doubled their zero-day usage (5 to 10 attributed zero-days year-over-year).



The Coruna iOS exploit kit (259 articles, the fifth most-covered story), documented by GTIG and iVerify on 3 March, demonstrated the zero-day supply chain problem in practice. Five full exploit chains containing 23 exploits moved from a commercial surveillance vendor to Russian state espionage (UNC6353) to Chinese cybercrime (UNC6691) in under twelve months. Both GTIG and iVerify linked Coruna's exploit techniques to Operation Triangulation (12 mentions in Q1), the campaign Kaspersky attributed to US intelligence in 2023. The connection, if accurate, means government-grade exploit capabilities are proliferating through commercial markets into criminal hands within a year of deployment.

Coruna iOS Exploit Kit Targets Multiple Threat Actors

261 articles / 164 sources

https://threatcluster.io/cluster/2df66b07

Supply chain acceleration

Supply chain attack mentions rose 30% quarter-over-quarter (257 to 334). The npm and Python package ecosystems were under sustained attack throughout Q1.

Incident	Score	Detail
Pawn Storm / PRISMEX Ukraine	77.85	Defence sector supply chain
NPM PylangGhost RAT	77.00	Malicious npm packages
NK Polyfill Attack	75.60	100K websites affected
China Compromises Notepad++ Updates	75.50	Update infrastructure
Glassworm npm Supply Chain	75.00	React Native packages
TeamPCP Telnyx SDK	72.75	Python SDK compromise
FCC Bans Foreign Routers	73.25	Hardware supply chain, 36 articles
LiteLLM Compromised	72.00	AI infrastructure, 29 articles
Trivy Scanner Compromised	72.00	Security tooling, 26 articles

TeamPCP emerged as a dedicated supply chain threat actor, compromising both the Telnyx Python SDK and the LiteLLM AI proxy framework. The targeting of LiteLLM is significant: it is a widely used abstraction layer for interacting with multiple LLM APIs. Compromising it provides access to API keys, prompts, and responses flowing through the proxy.

The Trivy vulnerability scanner compromise represents supply chain attacks targeting security tooling directly. When the tools used to detect vulnerabilities are themselves compromised, the detection pipeline is poisoned at source.

The North Korean Polyfill.io supply chain attack affected approximately 100,000 websites, continuing Pyongyang's pattern of large-scale web infrastructure compromise for both revenue generation and access.

A Chinese state actor compromised the Notepad++ update infrastructure, targeting a text editor used globally by developers and system administrators.

The attack exploits the implicit trust users place in software update mechanisms.

The FCC banned foreign-made consumer routers (36 articles, score 73.25), a policy response to the hardware supply chain risk that Chinese-manufactured networking equipment poses to US infrastructure.

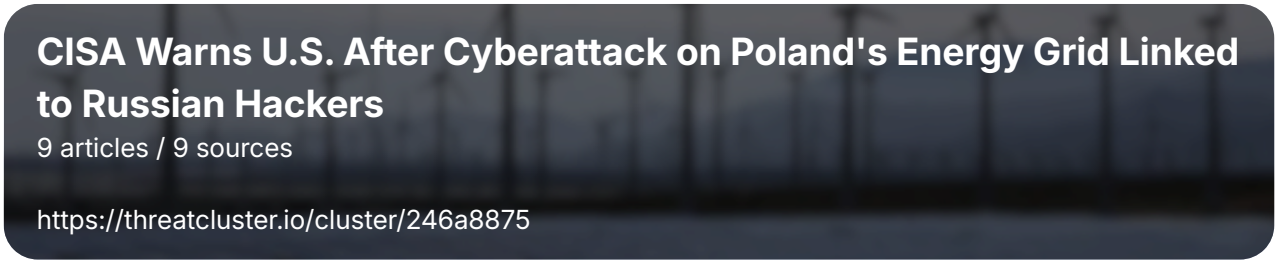


The Poland energy grid attack

The Russian cyberattack on Polish energy infrastructure scored 92.49, making it the ninth highest-scored cluster of the quarter. Russian actors compromised 30+ wind and solar farm sites using default passwords.

Poland's mention count rose from 37 (Q4) to 136 (Q1), a 268% increase driven primarily by this incident. The attack is a case study in OT security underinvestment. No MFA. Outdated equipment. Passwords still set to factory defaults. While IT security receives budget and tooling, operational technology networks in the renewable energy sector run on legacy systems with minimal staff and deferred maintenance.

The incident ties directly to the energy sector's 113% increase in Q1 targeting. As Europe accelerates renewable infrastructure deployment, the attack surface expands without corresponding security investment. Adversaries know this.



Malware trends

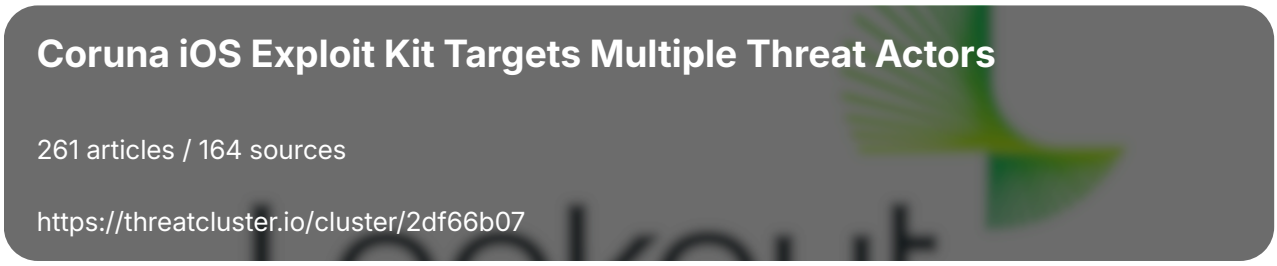
Top 10 malware families

Rank	Malware	Q1 mentions	Trend (J/F/M)	Type
1	React2Shell	47	20 / 16 / 11	RCE
2	Kimwolf	40	15 / 7 / 18	Backdoor
3	Predator	37	2 / 31 / 4	Spyware
4	Coruna	36	0 / 0 / 36	iOS exploit kit
5	Aisuru	33	10 / 6 / 17	Botnet
6	VoidLink	28	20 / 6 / 2	Fading
7	ClickFix	27	9 / 11 / 7	Social engineering
8	Pegasus	27	7 / 16 / 4	Spyware
9	Cobalt Strike	22	7 / 11 / 4	Red team / adversary
10	Glassworm	20	5 / 4 / 11	Supply chain

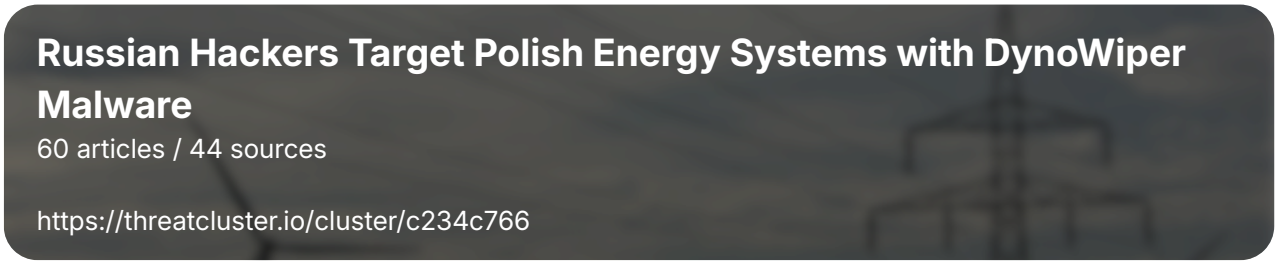
New malware families

511 new malware families were first tracked in Q1 2026. The most significant:

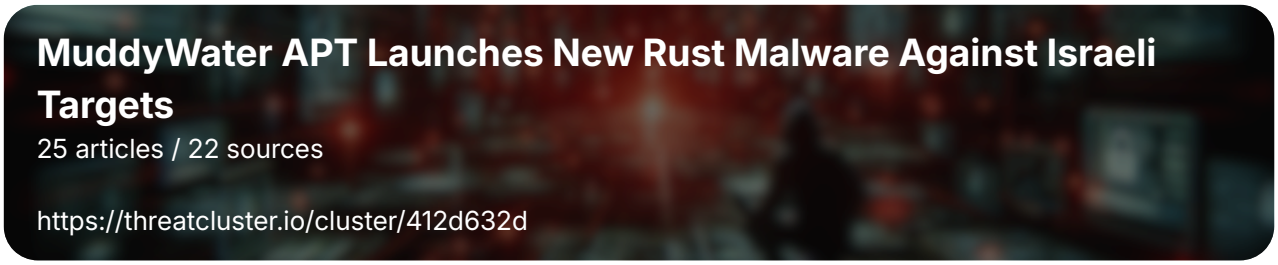
Coruna (36 mentions, March only): iOS exploit kit documented by Google GTIG and iVerify. Five full exploit chains, 23 exploits, targeting iOS 13 through 17.2.1. Moved from surveillance vendor to Russian espionage to Chinese cybercrime within twelve months. ThreatCluster tracked Coruna from its first public mention on 3 March.



DynoWiper (13 mentions, new): Wiper malware linked to geopolitical escalation. Consistent with Iranian destructive TTPs historically seen in campaigns against Saudi Aramco (Shamoon, 2012), Albanian government (HomeLand Justice, 2022), and Israeli targets.



RustyWater (7 mentions, new): Rust-based RAT deployed by MuddyWater (MOIS-affiliated) against Israeli government, military, and financial targets. Represents MuddyWater's continued evolution through programming languages (PowerShell to Python to .NET to Golang to Rust).



PromptSpy (17 mentions, February only): AI-themed spyware that appeared and vanished within a single month.

Brickstorm (19 mentions, growing: 1 to 7 to 11): Chinese backdoor with sustained month-over-month growth. Worth monitoring into Q2.

AI-themed malware

A new category of malware using AI branding entered the ecosystem:

- PromptSpy: 17 mentions (spyware)
- PromptLock: 6 mentions (ransomware)
- AiLock: 4 mentions (ransomware)

The naming convention exploits current market interest in AI. Open-source reporting does not confirm whether these tools incorporate actual AI capabilities or use the branding for marketing purposes.



Infostealer market churn

The infostealer landscape reshuffled significantly:

Infostealer	Q4 2025	Q1 2026	Direction
Rhadamanthys	40	6	Collapsed
VenomRAT	29	1	Near-extinct
Lumma Stealer	26	11	Halved
RedLine	4	17	Growing
VVS Stealer	0	10	New
AMOS (macOS)	—	10	Sustained

The decline of established infostealers alongside the growth of RedLine and new entrants indicates market rotation rather than reduced demand. Stolen credentials continue to feed the broader cybercrime ecosystem, as evidenced by the LeakBase forum (142,000 members) before its seizure in March.

Disappeared malware

Several malware families active in Q4 vanished entirely: Landfall (45 to 0), Sturnus (27 to 0), Elysium (24 to 0), Sesameop (20 to 0), DroidLock (17 to 0), Ngate (12 to 0), EdgeStepper (11 to 0), Badcandy (11 to 0), Junction (11 to 0), MacSync Stealer (10 to 0), GuestConduit (10 to 0).

AI as an attack surface

Agentic AI governance was the most-covered story of Q1 2026 with 752 articles. That volume reflects the industry's awareness that AI is creating new attack surfaces faster than security frameworks can address them.

AI as a tool

Chinese cyberspies leveraged Claude AI for automated attack operations (score 72.5). Lazarus Group used deepfake technology in targeted attacks (score 72.5). State actors deployed AI-generated misinformation during the Iran war (score 72.25). Armis reported a 100% failure rate in AI-generated secure code, raising questions about the reliability of AI-assisted development in security contexts.

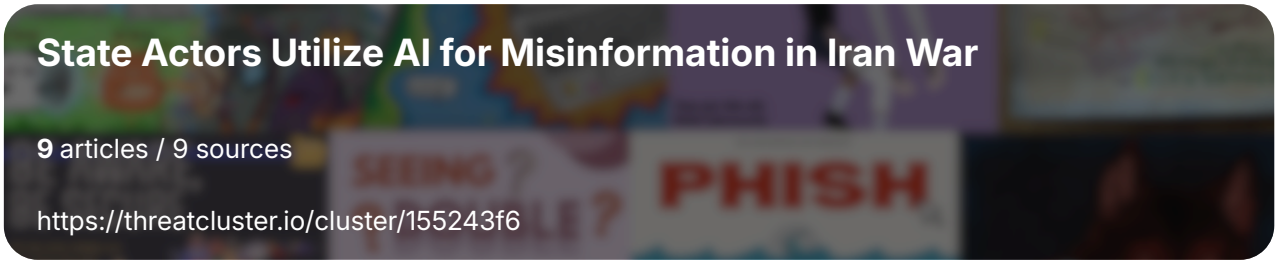
Chinese Cyberspies Leverage Claude AI for Automated Cyberattacks
2 articles / 2 sources

https://threatcluster.io/cluster/49430e56

Lazarus Group Uses Deepfake in Targeted Attack on AllSecure CEO

1 articles / 1 sources

https://threatcluster.io/cluster/ac4841df



State Actors Utilize AI for Misinformation in Iran War

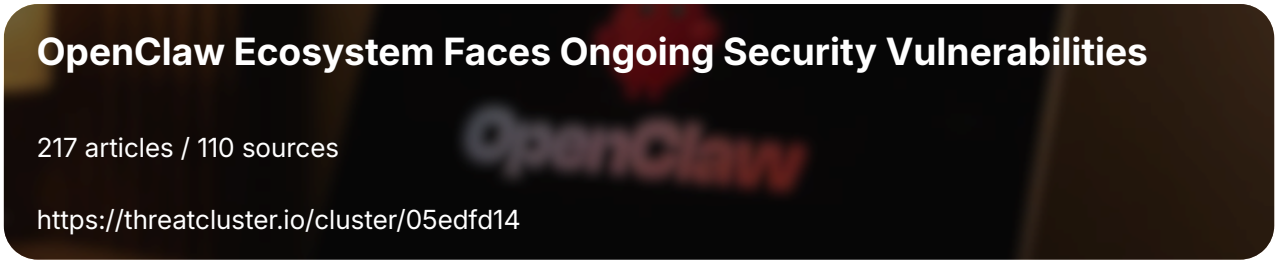
9 articles / 9 sources

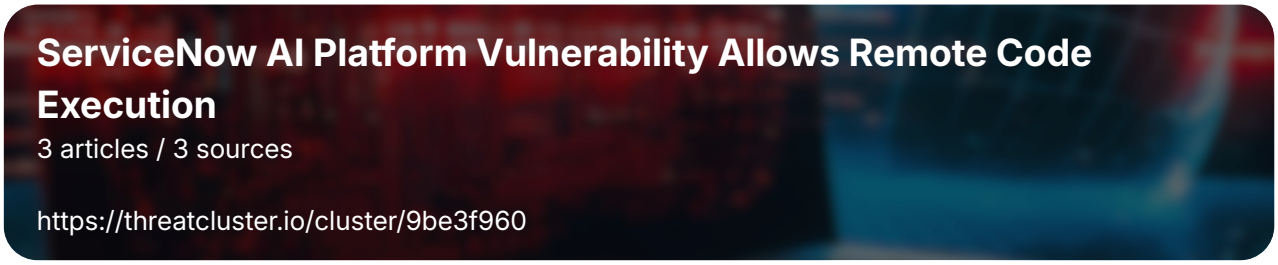
https://threatcluster.io/cluster/155243f6

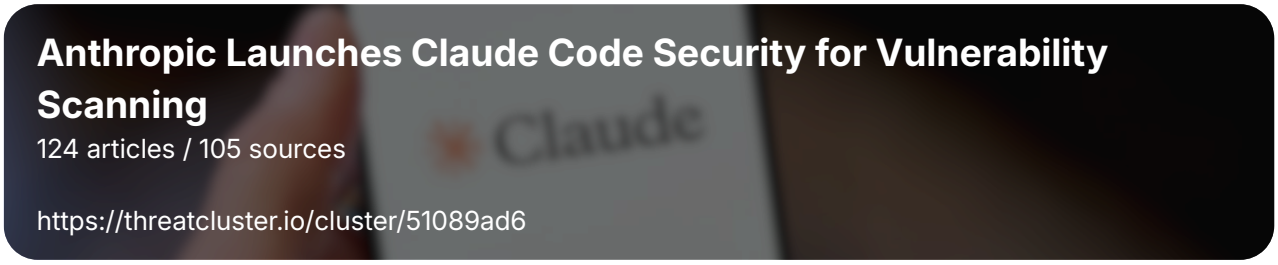
threatcluster.io
hello@threatcluster.io
71-75 Shelton Street, Covent Garden, London, WC2H 9JQ

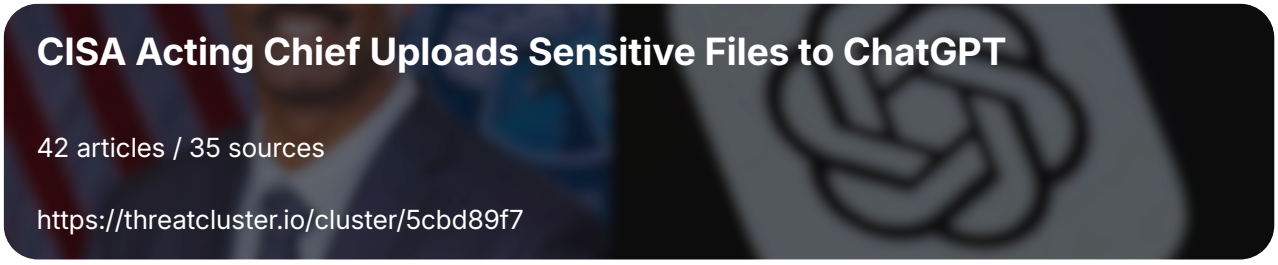
AI as a target

The LiteLLM supply chain compromise targeted AI proxy infrastructure directly. OpenClaw vulnerabilities generated 216 articles (the seventh most-covered story). ServiceNow's AI Platform had a critical RCE vulnerability (score 75.51). Anthropic Claude Code security generated 124 articles, reflecting both the rapid adoption of AI development tools and the security concerns they raise. ChatGPT appeared in 61 platform mentions across Q1, including the incident where the acting CISA head uploaded sensitive government documents to the public service.



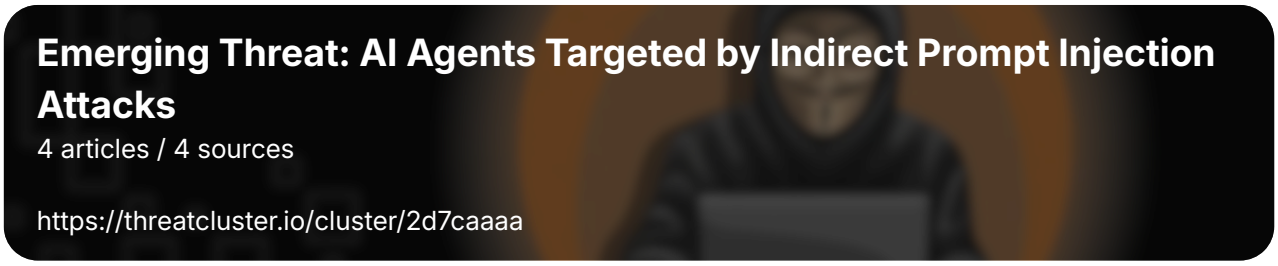






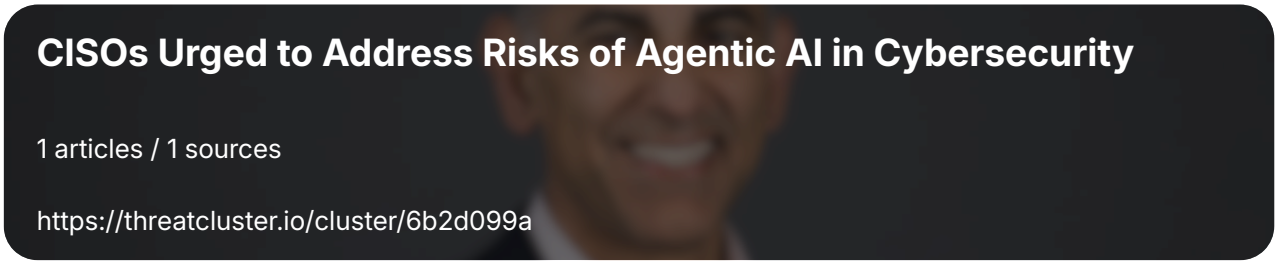
AI agents

AI agent security received dedicated coverage (score 71.75), with indirect prompt injection identified as the primary attack vector. CISOs were urged to address agentic AI risks as autonomous AI tools gain access to calendars, emails, files, and APIs. The convergence is clear. AI is simultaneously a tool for attackers, a target for compromise, and an attack surface that organisations are expanding voluntarily.



Emerging Threat: AI Agents Targeted by Indirect Prompt Injection Attacks
4 articles / 4 sources

https://threatcluster.io/cluster/2d7caaaa



CISOs Urged to Address Risks of Agentic AI in Cybersecurity

1 articles / 1 sources

https://threatcluster.io/cluster/6b2d099a

Platform targeting

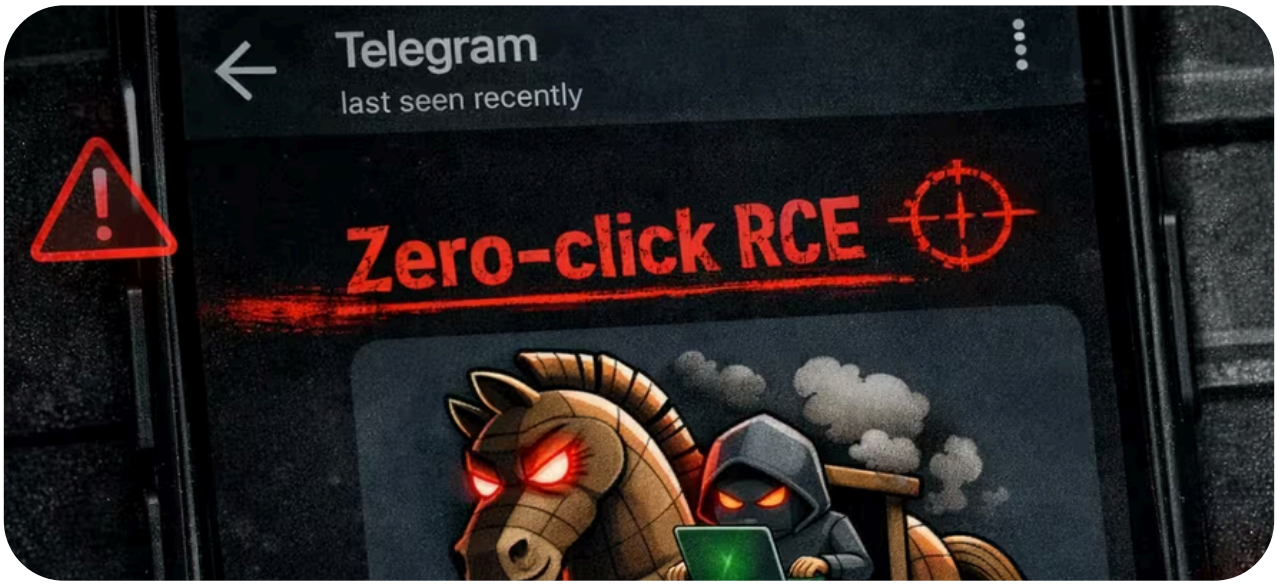
Rank	Platform	Q1 mentions
1	Windows	754
2	Android	312
3	Linux	281

Rank	Platform	Q1 mentions
4	iOS	169
5	macOS	162
6	Telegram	137
7	WhatsApp	125
8	GitHub	113
9	Instagram	68
10	Microsoft 365	66

Windows dominates at 754 mentions, more than double Android (312). The mobile split favours Android (312) over iOS (169), though the Coruna iOS exploit kit's March spike (36 mentions) and Pegasus's sustained activity (27) indicate iOS is not being ignored.

The messaging platform numbers tell a specific story. Telegram at 137 mentions reflects both its role as a hacktivist coordination platform (Electronic Operations Room, 60+ Iran-aligned groups) and the Telegram zero-day (score 76.5). WhatsApp at 125 mentions ties directly to the Dutch MIVD/AIVD disclosure of Russian state-sponsored account hijacking. These are not just communication platforms. They are operational infrastructure for both attackers and the officials being targeted.

GitHub at 113 mentions reflects its role in supply chain attacks (Glassworm, Polyfill, malicious npm packages) and as a distribution mechanism for malware. ChatGPT at 61 and OpenClaw at 58 confirm AI platforms as an emerging target category.



Industry and geopolitical targeting

Industries

Rank	Industry	Q1 2026	Q4 2025	Change
1	Government	654	492	+33%
2	Healthcare	332	246	+35%
3	Financial	318	333	-5%
4	Energy	281	132	+113%

Rank	Industry	Q1 2026	Q4 2025	Change
5	Manufacturing	175	174	Flat
6	Telecommunications	160	76	+111%
7	Technology	133	120	+11%

Energy's 113% growth and telecommunications doubling are directly attributable to the Iran conflict and Salt Typhoon's sustained operations respectively.

Healthcare's 35% rise reflects both the Stryker wiper attack and broader ransomware targeting of medical infrastructure. Retail dropped 45%, suggesting either reduced targeting or reduced reporting. Aerospace appeared at 11 mentions, a sector worth monitoring given APT33's documented focus on aviation and defence industrial base targets.

Geopolitical shifts

Country	Q4 2025	Q1 2026	Change
Iran	121	808	+568%
Israel	45	356	+691%
United States	334	603	+81%
Ukraine	117	356	+204%

Country	Q4 2025	Q1 2026	Change
Russia	345	565	+64%
China	383	550	+44%
Poland	37	136	+268%
Qatar	5	76	+1,420%
Kuwait	6	57	+850%
Bahrain	0	50	New entrant

Nation-state cluster attribution

Attribution	Clusters	Avg score
Iran	225	57.1
China	147	47.0
Russia	143	51.1
North Korea	57	45.7

Iran's 225 attributed clusters at an average score of 57.1 (higher than any other nation-state) confirm both the volume and severity of Iranian cyber activity in Q1.

Russia maintains the second-highest average score (51.1), reflecting the quality of its operations even as overall volume sits below China's cluster count.

North Korea's 57 clusters at the lowest average score (45.7) aligns with the quieter quarter noted in the APT section.

MITRE ATT&CK and attack vector analysis

Rank	Technique	Q1 mentions
1	T1566 Phishing	1,009
2	T1041 Exfiltration Over C2 Channel	420
3	T1566.002 Spearphishing Link	254
4	T1071 Application Layer Protocol	237
5	T1059 Command and Scripting Interpreter	207
6	T1567 Exfiltration Over Web Service	199
7	T1486 Data Encrypted for Impact	148
8	T1068 Exploitation for Privilege Escalation	140
9	T1190 Exploit Public-Facing Application	138
10	T1195 Supply Chain Compromise	136

Phishing (T1566) dominates at 1,009 mentions, more than double the next technique.

T1190 (Exploit Public-Facing Application) at 138 mentions reflects the Cisco zero-day pattern and broader targeting of edge infrastructure.

T1195 (Supply Chain Compromise) at 136 mentions aligns with the npm/Python ecosystem attacks and the Coruna exploit kit proliferation.

T1059.001 (PowerShell) at 123 mentions remains a persistent execution mechanism across multiple campaigns.

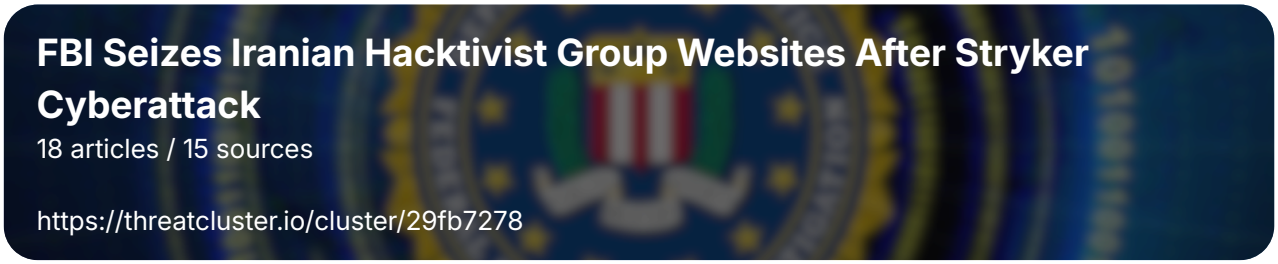
T1486 (Data Encrypted for Impact) at 148 mentions tracks the ransomware landscape, though the emergence of wiper malware (DynoWiper) means destructive operations are not captured by this technique alone.

Attack type distribution

Attack type	Q1 total	Q4 total	Change
Data Breach	2,423	2,207	+10%
Malware	2,194	1,811	+21%
Phishing	1,757	1,247	+41%
Ransomware	1,253	1,203	+4%
Zero-day Exploit	922	413	+123%

Attack type	Q1 total	Q4 total	Change
DDoS	540	279	+94%
Supply Chain	334	257	+30%
Botnet	111	74	+50%

Zero-day exploitation more than doubled. DDoS nearly doubled, driven by hacktivist activity during the Iran conflict. Supply chain attacks rose 30%. Botnet mentions (111) are notable given Aisuru's resurgence in March (17 mentions).



Campaigns

Campaign	Q1 mentions
Operation Epic Fury	37
Operation Cyber Guardian	20
Operation Synergia III	15

Campaign	Q1 mentions
Operation Zero	13
Operation Triangulation	12
Operation Neusploit	10
Pwn2Own Automotive 2026	9
Contagious Interview	8
Project Compass	7
Operation Atlantic	7
Operation Endgame	6
Operation Winter Shield	6

Operation Epic Fury (37 mentions) dominates, reflecting the US-Israel strikes on Iran. Operation Cyber Guardian (20) reflects Singapore's telco eviction. Operation Synergia III (15) was an Interpol-led international operation targeting cybercrime infrastructure.



Operation Triangulation (12 mentions) is notable for its connection to the Coruna iOS exploit kit. Both GTIG and iVerify identified shared exploit techniques between Coruna and the original Operation Triangulation campaign that Kaspersky disclosed in 2023 and the Russian government attributed to US intelligence. If the lineage holds, it means exploit capabilities originally deployed in a state intelligence operation are now circulating in the commercial surveillance market and criminal ecosystem within three years.

Contagious Interview (8 mentions) continues as a North Korean campaign using fake job interview processes to deliver malware, one of the few DPRK operations that maintained visibility in an otherwise quiet quarter.



IOCs and technical indicators

IOC type	Unique	Mentions
Domains	605	826
MD5	103	105
SHA1	77	88

IOC type	Unique	Mentions
SHA256	75	86
IPv4	46	61
ETH addresses	5	6
XMR addresses	3	3
BTC addresses	1	1

3,306 unique CVEs were tracked in Q1. The most referenced: CVE-2026-20127 (36 mentions), CVE-2026-20805 (35), CVE-2026-21509 (35, Microsoft Office zero-day), CVE-2026-20131 (17, Cisco FMC, exploited by Interlock ransomware), and CVE-2026-20045 (14, Cisco Unified CM zero-day).

The cryptocurrency IOC data is small in volume but tells a story about payment methods. 5 Ethereum addresses, 3 Monero (XMR), and 1 Bitcoin. Monero's presence alongside Ethereum reflects ransomware operators' growing preference for privacy coins alongside traditional cryptocurrency payment rails. Anyone conducting financial tracing on ransomware payments should account for both.



Law enforcement operations

Q1 2026 saw significant law enforcement action against cybercrime infrastructure.

Operation Leak (3-4 March): FBI and Europol seized LeakBase, a stolen credential marketplace with 142,000 registered members and over 215,000 private messages.

13 arrests across 14 countries. 37 of the most active users targeted with enforcement actions. FBI Assistant Director Brett Leatherman described LeakBase as "a place where users were increasingly sharing information to access US networks, potentially critical infrastructure."

KELA noted the forum prohibited data related to Russian entities, indicating Russian-based or Russian-protected administrators.



Tycoon2FA disruption (March): Microsoft and Europol seized 330 domains belonging to the phishing-as-a-service platform. Tycoon2FA accounted for 62% of all phishing attempts blocked by Microsoft in mid-2025, with over 30 million emails intercepted in a single month. The takedown disrupted the service layer connecting phishing kit operators to credential marketplaces like LeakBase.



Operation Synergia III (15 mentions): Interpol-led operation targeting cybercrime infrastructure across multiple jurisdictions.

Phobos prosecution: The Phobos ransomware leader pleaded guilty, facing up to 20 years in prison. Phobos generated 17 mentions in Q1, primarily in February (9) and March (8).

Operation Cyber Guardian (20 mentions): Singapore's 11-month, 100+ personnel operation to evict UNC3886 from national telecommunications infrastructure.

Taking LeakBase and Tycoon2FA out in the same week was not coincidental. Tycoon2FA generated the stolen credentials. LeakBase sold them. Removing both disrupts the supply chain from phishing kit to credential marketplace to initial access.

Outlook: Q2 2026

Based on Q1 data, six trends will shape the remainder of 2026.

Iranian cyber operations will intensify and become less predictable.

The command-and-control relationship between IRGC/MOIS headquarters and their cyber operators has been disrupted by the decapitation of senior leadership and near-total internet blackout. Handala's trajectory from data leaks to Fortune 500 wiper attacks to the FBI Director's email in a single month demonstrates rapid capability escalation.

With 225 attributed clusters in Q1 and the conflict ongoing, Iranian-linked activity will remain elevated. The question is whether proxy groups operating with increased autonomy will expand targeting beyond current patterns.



The ransomware fragmentation will accelerate.

88 new groups in Q1. Established operators collapsing. Interlock's model (build around a specific vulnerability rather than maintaining broad access) will be replicated. Expect more groups tied to specific zero-days or exploit chains, shorter operational lifespans, and faster cycling through the ecosystem. The barrier to entry is now a zero-day and a Telegram channel.

Cisco infrastructure will remain under sustained attack.

Five zero-day clusters in a single quarter against a single vendor is not coincidence. The SD-WAN vulnerability exploited since 2023 suggests deep, ongoing access that has not been fully remediated. The March patch bundle (48 vulnerabilities) closed known gaps but the pattern of discovery suggests more will follow.

AI infrastructure will become a primary supply chain target.

LiteLLM and OpenClaw were the beginning. As organisations deploy AI agents with access to internal systems, APIs, and data, compromising the AI middleware layer (proxy frameworks, orchestration tools, model serving infrastructure) provides access to everything downstream. The 752-article volume around agentic AI governance reflects the industry recognising this risk. The supply chain attacks on AI tooling demonstrate that threat actors have already identified it.

North Korean activity warrants close monitoring.

The collective decline across all DPRK-linked APT groups in Q1 is anomalous and unexplained. Lazarus, Kimsuky, Konni all declining. APT38 disappeared entirely. Quiet from North Korean groups historically precedes capability development or retooling. If DPRK operations resume at scale in Q2, the gap in Q1 may represent preparation rather than retreat.



Subsea cable and telecommunications infrastructure faces physical and cyber convergence.

The simultaneous closure of the Red Sea and Strait of Hormuz to commercial traffic, combined with GPS spoofing affecting 1,650+ vessels, creates conditions where accidental damage to submarine cable infrastructure becomes increasingly probable. The 113% increase in energy sector targeting and the doubling of telecommunications mentions in Q1 reflect the broader trend of critical infrastructure moving from secondary to primary targeting.

Methodology

ThreatCluster aggregates open-source intelligence from 8,500+ monitored sources including RSS feeds, government advisories (CISA, NCSC, ENISA, CERT-AU), vendor security blogs, news outlets, social media (X, Reddit, LinkedIn), dark web forums, and ransomware leak sites. The top source (Microsoft MSRC) accounts for only 3.9% of total volume, ensuring no single source dominates the dataset.

Articles are embedded using transformer-based models and clustered using DBSCAN (Density-Based Spatial Clustering of Applications with Noise) to group related reporting by semantic meaning rather than keyword matching. This approach produces a clustering ratio of 8.7:1 (improved from 6.3:1 in Q4), meaning each cluster represents an average of 8.7 source articles reporting on the same underlying story. At 603 articles per day, that equates to approximately 69 actionable clusters daily, a reduction of over 17 hours of manual reading at an estimated 2 minutes per article.

Structured entities are extracted automatically from clustered articles using a combination of named entity recognition, regular expression matching, and LLM-enhanced extraction for complex entities (MITRE ATT&CK techniques, threat actor attribution, campaign linkage). Entity types include threat actors, malware families, CVEs, IOCs (domains, IPs, hashes, cryptocurrency addresses), MITRE ATT&CK techniques, industries, countries, platforms, and tools.

threatcluster.io
hello@threatcluster.io
71-75 Shelton Street, Covent Garden, London, WC2H 9JQ

In Q1 2026, the platform tracked 11,668 unique entities and identified 3,060 new CVEs, 511 new malware families, and 230 new APT groups first seen during the quarter.

Threat scores are calculated on a 0-100 scale combining severity, geopolitical significance, actionability, and sentiment analysis. Scores are weighted toward actionability and severity. Only 35 clusters (0.6%) scored 80 or above in Q1, each corresponding to a confirmed high-impact incident.

ThreatCluster tracks both emerging and declining entities. Identifying that a previously active malware family or APT group has disappeared from open-source reporting is treated as an intelligence signal equivalent to identifying a new entrant. Disappearance may indicate improved operational security, rebranding, disruption, or operational cessation.

All data in this report covers the period 1 January to 27 March 2026. Historical comparisons reference Q4 2025 (October to December 2025). Percentages are rounded to the nearest whole number unless otherwise stated.

threatcluster.io
hello@threatcluster.io
71-75 Shelton Street, Covent Garden, London, WC2H 9JQ



Every entity, cluster, and data point referenced in this report is searchable on the platform. The Q1 2026 dataset comprises 53,062 articles clustered into 6,092 intelligence groups across 6,753 sources.

© 2026 ThreatCluster Ltd. Registered in England and Wales.

ThreatCluster — threatcluster.io