ANALYST USE | EDP MONTHLY CYBERCRIME ECOSYSTEM INTELLIGENCE REPORT | APRIL 2026

MONTHLY CYBERCRIME ECOSYSTEM INTELLIGENCE REPORT

Coverage Period: April 2026 | Classification: ANALYST USE

Produced by: EDP Intelligence Cell | Date: April 30, 2026

SECTION 1 — EXECUTIVE SUMMARY

Five highest-priority ecosystem-level developments, ranked by strategic impact. Each item carries a confidence label and at least one supporting metric.

1. Vect RaaS formalized an unprecedented mass-affiliate partnership with BreachForums on April 16, 2026, distributing functional affiliate keys to all 300,000+ registered forum members and embedding the forum directly into the ransomware execution pipeline — representing the largest documented single-event expansion of the ransomware affiliate pool in the history of RaaS. **[CONFIRMED]**

2. The EU's 20th Russia sanctions package (April 23, 2026) imposed a total ban on Russian crypto platforms and blocked the digital ruble and RUBx stablecoin, effective May 24, 2026, applying the most comprehensive single regulatory constraint on ransomware money-laundering infrastructure since Garantex sanctions in 2022. **[CONFIRMED]**

3. Analysis of The Gentlemen's SystemBC C2 infrastructure revealed 1,570+ victims, approximately 5x the group's published leak-site count of 320, confirming that declared victim counts systematically undercount actual operational reach across the ransomware ecosystem. **[CONFIRMED]**

4. Active data-leak sites reached a record 91 in Q1 2026 alongside 2,638 published victim posts — a 22% increase over Q1 2025 — with ecosystem fragmentation accelerating following RAMP's FBI seizure (January 28, 2026), indicating disruption of central coordination nodes is driving proliferation rather than contraction. **[CONFIRMED]**

5. The FBI IC3 2025 Annual Report (released April 6, 2026) recorded $20.877 billion in cybercrime losses — a 26% year-over-year increase and first crossing of the $20B threshold — with ransomware continuing to drive critical infrastructure targeting that intensified in Q1 2026. **[CONFIRMED]**

SECTION 2 — RANSOMWARE ECOSYSTEM — MONTHLY STATISTICS

Coverage: April 2026 (partial April data supplemented by Q1 2026 and March 2026 final figures where April monthly totals are still accumulating as of April 30). All figures sourced from Ransomware.live, Breachsense, ReliaQuest, and ZeroFox reporting unless noted.

Core Statistics

Total victims disclosed (March 2026, confirmed final): 808 — Source: Breachsense March 2026 Ransomware Report

April 2026 victim count (partial, as of April 28): ~760 projected; ransom-db weekly data shows Qilin 107, TheGentlemen 70, Akira 69 in rolling 30-day window

Active group count (Q1 2026): 70 groups tracked by Ransomware.live; 65 groups in March per Breachsense; 91 active leak sites (record)

New groups identified (Q1 2026): Multiple entrants including Orion ransomware, 0APT, and Vect (December 2025 RaaS debut)

Defunct or dormant groups: RAMP forum seized January 28, 2026; associated affiliate channels disrupted; successor forums emerging

Q1 2026 total posts on leak sites: 2,638 — up 22% from Q1 2025 (2,161) — Source: ReliaQuest

Month-over-month victim change (Feb to March 2026): +19% (March 808 vs. February ~679)

Estimated ransom volume: No reliable aggregate monthly data available. FBI IC3 2025 full-year: $20.877B total cybercrime losses.

Sector Targeting Trend Table — March 2026

Sector	March 2026 (n)	Prior Month (n)	% Change	Trend
Manufacturing	76	No prior data	N/A	Dominant — #1 sector Q1 2026 (419 incidents)
Construction	53	No prior data	N/A	Elevated — consistent top-5 position
Finance	48	No prior data	N/A	Elevated — top-3 March
Healthcare	18	No prior data	N/A	Stable — April 26 incidents confirmed in UK/US/AU
Government	14	No prior data	N/A	Stable — consistent mid-tier targeting

Note: Sector-level prior-month comparatives unavailable from accessible sources this cycle; noted per Rule 2.

Geographic Targeting Analysis

- United States: 50% of all March victims (404/808). April rolling data: 37% of tracked attacks — Source: Breachsense, ransom-db
- France: 36 victims (March); Germany: 32 victims (March) — Source: Breachsense
- Q1 2026: North America 54% of all incidents; US alone 51% (1,084 incidents) — Source: ZeroFox Q1 2026 Ransomware Wrap-Up

- CIS-exclusion patterns: Assessed to be holding for most established RaaS groups (Qilin, Akira). Vect exclusion behavior: Unknown — no confirmed CIS targeting or explicit exclusion language documented as of April 30. The Gentlemen: Unknown CIS exclusion policy.
- EU targeting uptick noted in April: UK, Switzerland, Germany appeared in April 26 incident trackers alongside North American victims — Source: Purple Ops April 2026

Leak Site Three-Signal Composite

Signal	April 2026	Prior Period (Q1 2025)	Trend	Notes
Post Volume (victims published)	~760 projected (partial); March final: 808	Q1 2025: 2,161 total (avg 720/mo)	Increasing	22% YoY increase Q1 2026 vs Q1 2025; record 91 active sites
Time-to-Publish (avg days)	No reliable data available for this metric	No reliable data available for this metric	Unknown	Compression would indicate escalating pressure; data gap noted
Takedown/Relaunch Cycle	RAMP seized Jan 28; T1erOne and others emerged within 30 days	Post-LockBit: ~30-60 day reconstitution	Resilience increasing	Faster fragmentation than consolidation; 91 active sites vs. ~50 in mid-2024

Composite interpretation: Post volume and active site count are both increasing, indicating ecosystem expansion. The takedown-to-relaunch signal shows rapid reconstitution but into fragmented smaller operations rather than single successor entities. Divergence between declared victim counts (leak sites) and actual operational reach (The Gentlemen C2 analysis: 1,570 actual vs. 320 published) is analytically significant — lean-site post volume likely undercounts true operational impact by a factor of 3-5x.

SECTION 3 — THREAT ACTOR LANDSCAPE

Russia/CIS-linked groups prioritized. April 2026 victim counts are rolling 30-day figures from ransom-db weekly reporting (as of April 28, 2026). CIS exclusion assessments based on available intelligence.

Priority Threat Actors — April 2026

QILIN (Agenda)

April victims (rolling 30-day): 107 — Source: ransom-db April 24, 2026 weekly report; 31 confirmed in final week of April alone

Q1 2026 total: 338 victims — #1 most active group Q1 2026 — Source: ZeroFox, ReliaQuest

Record performance: March 2026: 131 victims — highest single month for any group in Q1 2026 — Source: Breachsense

Cumulative known proceeds: No reliable figure publicly available

Key development (April): Maintained dominance representing approximately 14% of all tracked ransomware activity in rolling 30-day window

Threat level vs. prior month: Increasing — three consecutive months above 100 victims

CIS exclusion: Assessed (consistent with Russia/CIS-linked operational patterns; no confirmed CIS victim targeting documented)

THE GENTLEMEN (The_Gentelman)

April victims (rolling 30-day): 70 — Source: ransom-db April 2026

Q1 2026 total: 192 victims — #3 most active Q1 2026; 588% QoQ growth (26 posts Q4 2025 to 179 Q1 2026) — Source: ReliaQuest

Actual operational scale: 1,570+ victims identified via SystemBC C2 server analysis (April 21, 2026) — Source: Check Point Research / The Hacker News

Cumulative since emergence (July 2025): 320+ published victims; 1,570+ actual C2-identified victims

Key development (April): SystemBC C2 infrastructure exposed by researchers on April 21, revealing true victim scale 5x the published count; GPO abuse documented as domain-wide compromise mechanism

Technical indicators: SystemBC proxy malware (SOCKS5 tunneling, custom RC4-encrypted C2); Cobalt Strike; GPO-based lateral movement; internet-facing service exploitation for initial access

Threat level vs. prior month: Increasing — infrastructure revelation confirms larger operational footprint than disclosed

CIS exclusion: Unknown — no confirmed policy

AKIRA

April victims (rolling 30-day): 69 — Source: ransom-db April 2026

Q1 2026 total: 197 victims — #2 most active Q1 2026 — Source: ZeroFox

Cumulative known proceeds: Estimated $42M+ (FBI advisory, prior periods; no updated April 2026 figure available)

Key development (April): Maintained consistent mid-market targeting presence; no major structural changes reported

Threat level vs. prior month: Stable — consistent high-volume operation

CIS exclusion: Assessed — consistent historical pattern

VECT (New Entrant — High Priority)

April victims (rolling 30-day): No reliable data — victim pipeline just activating post-April 16 key distribution

Debut: December 2025 on Russian-language cybercrime forum

Affiliate model: Mass-open RaaS — BreachForums partnership April 16, 2026; 300,000+ potential affiliates via forum membership

Key development (April): April 16: Mass affiliate key distribution to entire BreachForums membership. April 28-29: Critical bug disclosed — VECT 2.0 irreversibly destroys files over 131KB on Windows, Linux, and ESXi, functioning as a wiper rather than a ransomware; affiliate confidence and payment recovery likelihood severely undermined.

TeamPCP alignment: Formal alignment announced; TeamPCP provides supply-chain sourced access (compromised security tooling) feeding Vect operations

Threat level vs. prior month: Increasing in scale potential; wiper bug is a structural constraint on monetization

CIS exclusion: Unknown — no documented policy

INC RANSOM and CL0P

Q1 2026 position: Both in top-5 Q1 2026 by victim count — Source: ReliaQuest, ZeroFox

Cl0p April activity: Continued supply-chain focused operations; no major new disclosures in available April sources

April victim counts: No reliable April-specific data available for either group this cycle

Data Extortion Trend (Encryption-Free)

- Europol IOCTA 2026 (released April 28, 2026) confirms the extortion model is shifting away from data encryption toward pure data theft — Source: Europol
- Q1 2026 total leak-site posts: 2,638 — the aggregate metric now includes both encryption-plus-extortion and encryption-free extortion; no reliable breakdown percentage available this cycle. Notation: No reliable data available for this metric (encryption-free vs. encryption share, April 2026).
- Named groups operating extortion-only: ShinyHunters (identity-first, SaaS-native data theft; no encryptor deployed); 0APT (emerging, claimed attacks without encryption evidence)
- Q1 2026 trend: Attackers avoiding encryption reduce forensic visibility and post-incident response options; analysts note defense blind spots as primary growth driver for this model — Source: ReliaQuest Q1 2026, Morphisec

SECTION 4 — INITIAL ACCESS & TTP EVOLUTION

Access Vector Ranking (Q1 2026, Most to Least Common)

- 1. Credential-based intrusion (stolen credentials from infostealer logs, IAB-purchased access) — Dominant vector Q1 2026 — Source: ReliaQuest, RAMP analysis
- 2. Internet-facing service exploitation (VPN, RDP, Citrix) — Confirmed for The Gentlemen, Akira, and multiple unnamed groups
- 3. Software supply chain compromise — Elevated in April 2026 (Axios npm, Bitwarden CLI, Vercel/Context.ai, SAP npm) — Source: CISA, Elastic, Endor Labs
- 4. Phishing/spearphishing — Persistent baseline; IC3 2025 reports phishing losses escalated from $70M to $215.8M year-over-year
- 5. CVE exploitation of unpatched systems — Documented for Apache ActiveMQ, Fortinet FortiClient EMS, Windows Shell vulnerabilities in April 2026

Significant TTP Developments

- The Gentlemen — GPO abuse: Group Policy Objects abused to achieve domain-wide compromise; SystemBC used as persistent SOCKS5 proxy; Cobalt Strike as post-exploitation framework. Scale: 1,570+ confirmed C2 victims — Source: Check Point, April 21, 2026.
- Vect — Mass affiliate mobilization: BreachForums-integrated operational infrastructure; escrow, key distribution, and coordination embedded directly in forum. Qualitative shift from traditional vetted-affiliate RaaS model to open-access. VECT 2.0 cross-platform targeting (Windows, Linux, ESXi) — Source: Cynet, Dataminr, April 2026.
- TeamPCP — Supply chain access sourcing: Compromised Checkmarx GitHub Actions, Open VSX plugins, and in April 2026, SAP npm packages; access provided to Vect affiliates. Attack surface: developer toolchains and open-source security tooling — Source: The Register, The Hacker News, CISA.
- APT28 — LNK file exploit chain: CVE-2026-32202 (Windows Shell) combined with CVE-2026-21513 deployed via malicious Windows Shortcut files; targeted Ukraine and EU nations; zero-click vector — Source: The Register, April 29, 2026.

IAB Market Indicators Table

Indicator	Current Period	Prior Period	Trend
Volume of corporate access listings	No reliable monthly count available	Elevated through RAMP (pre-seizure)	Fragmented post-RAMP seizure (Jan 28, 2026); migrating to T1erOne and private channels
Median access price	$1,295 (2024 full-year average)	$2,000-$3,500 (2022-2023 range)	Declining — ~60% price reduction vs. prior years; volume strategy dominant
Premium listing ceiling	$3,000 (typical)	$10,000+ (peak 2022)	Compressing — high-value listings moving to private negotiations
Most-targeted sectors (top 3)	Manufacturing, Finance, Healthcare	Manufacturing, Finance, Healthcare	Stable sector targeting pattern
Dominant access type	RDP (dominant) > VPN > Citrix — Source: RAMP historical analysis, Flare	RDP > VPN > Citrix	Stable — RDP remains primary; credential-based entry dominant

Indicator	Current Period	Prior Period	Trend
Notable marketplace events	RAMP seized January 28, 2026; T1erOne emerged as early successor; RAMP had 1,732 threads, 7,707 users, 340K IP records leaked	RAMP operational; active listings	Significant disruption to central IAB marketplace; ecosystem fragmented

Note: Infostealer-to-IAB pipeline — median time from Lumma/StealC infection to dark web credential listing: No reliable data available for this metric (timing data not available in accessible sources this cycle). Qualitatively, Vercel/Context.ai breach demonstrates that stealer-sourced OAuth tokens were operationalized within weeks of initial infection (Lumma infection ~February 2026; attack chain executed April 2026).

SECTION 5 — MALWARE & STEALER ECOSYSTEM

Active Families — Ranked by Distribution Volume

1. LummaC2 / Remus

Market share / volume: Lumma + successor Remus: estimated dominant share of infostealer market in early 2026; exact percentage No reliable data available for this metric (post-disruption figures not confirmed)

Distribution method (April 2026): Remus: EtherHiding (blockchain-based C2 resolution) replacing Steam/Telegram dead-drop resolvers; browser-centric credential, cookie, and crypto wallet theft

Notable development: Remus emerged February 2026 as 64-bit successor following Lumma takedown (May 2025) and developer doxxing (Aug-Oct 2025). Key innovation: EtherHiding C2 resolution significantly hardens infrastructure against traditional takedown methods. Remus campaigns active and scaling — Source: Gen Digital, SOC Prime, April 2026.

Disruption status: Lumma: Disrupted May 2025, recovered within weeks. Remus: Active, no disruption action.

2. StealC

Market share: Top-3 infostealer; combined Lumma+StealC+RedLine account for 75%+ of infections — Source: Breachsense

Distribution method: MaaS subscription model ($250/month entry); widespread loader and dropper distribution

Notable development: No major structural changes reported April 2026

Disruption status: Active — no disruption action

3. RedLine

Market share: Declining following Operation Magnus (October 2024); logs remain in circulation

Distribution method: Legacy logs still circulating through underground markets and Telegram channels

Notable development: Post-Magnus decline continues; logs from prior infections remain a live credential threat despite service disruption

Disruption status: Disrupted (Operation Magnus, Oct 2024); logs in ongoing circulation

4. ACRStealer / Vidar

Market share / volume: Active distribution in early 2026 alongside Lumma and StealC — Source: Breachsense malware trends report

Distribution method: Loader networks; phishing chains

Notable development: No specific April 2026 developments identified in accessible sources

Disruption status: Active — no disruption action

Infostealer-to-IAB Pipeline Assessment

- Scale context: 3.9 billion credentials compromised across 4.3 million devices in 2024; average 1,861 cookies per infection enabling MFA bypass via session token theft — Source: Breachsense, Darktrace
- Pipeline integrity: A single unprotected database discovered January 2026 contained 149 million stolen login/password pairs including 48 million Gmail accounts, confirming that credential stockpiles significantly exceed what is actively listed on IAB markets at any given time — Source: AlgeriaTech News
- Pipeline timing: Vercel/Context.ai case demonstrates a multi-week operational gap between initial stealer infection and weaponization of stolen OAuth tokens. Lumma Stealer infection at Context.ai occurred approximately February 2026; credential weaponization executed April 2026 (approximately 8-10 week lag in this documented case) — Source: Trend Micro, April 2026.

- Operational significance: EtherHiding adoption by Remus reduces law enforcement's ability to sinkhole C2 infrastructure, extending the operational life of stealer deployments and the credential pipeline feeding IAB markets.

SECTION 6 — FINANCIAL & INFRASTRUCTURE SIGNALS

Sanctions and Enforcement Actions — April 2026

Action 1: OFAC Southeast Asia Scam Center Designations

Designating authority: OFAC (U.S. Department of the Treasury)

Date: April 23, 2026

Target: 29 entities in Cambodia; centered on Senator Kok An, associate Rithy Raksmei, and network of casinos/hotels/holding companies

Stated rationale: Money laundering of cyber-enabled fraud proceeds; support for Southeast Asian scam center infrastructure

Financial exposure: $701.9 million in cryptocurrency restrained — Source: Chainalysis, April 2026

Assessed disruption impact: Medium — targeted specific Cambodian network; primary nexus is fraud/BEC rather than ransomware; crypto restraint is significant but scam center operators have demonstrated geographic mobility

Action 2: EU 20th Russia Sanctions Package — Crypto Provisions

Designating authority: European Union Council

Date: April 23, 2026; effective May 24, 2026

Target: All Russian and Belarusian crypto platforms; digital ruble (CBDC); RUBx stablecoin; 20 Russian banks; 4 third-country financial institutions (SPFS-linked); Kyrgyz exchange TengriCoin

Stated rationale: Sanctions evasion; support for Russia's war economy; crypto circumvention of prior EU financial restrictions

Financial exposure: Russia's A7A5 ruble-backed token has processed an estimated $93.3 billion in sanctions evasion — Source: Chainalysis 2026 Crypto Crime Report

Assessed disruption impact: High (structural, 90+ days) — Total ban on Russian crypto platforms closes the most accessible EU-connected laundering channels; effective May 24 deadline creates a 31-day adjustment window during which displacement to non-EU-compliant exchanges is expected

Action 3: Grinex Exchange Hack / Operational Suspension

Status: Not a sanctions action — criminal/technical incident

Date: April 15, 2026

Event: Sanctioned Russian crypto exchange Grinex (OFAC-designated Garantex successor) was hacked and lost $13.7 million; suspended operations attributing attack to Western special services — Source: Breached.Company

Assessed impact: Medium — Grinex suspension removes a designated ransomware money-laundering node; Russian cybercriminals will migrate to remaining non-designated exchanges and over-the-counter brokers

Financial Flow Observations

- Illicit cryptocurrency addresses received at least $154 billion in 2025 — Source: Chainalysis 2026 Crypto Crime Report (ANALYST INFERENCE confidence on ransomware-specific portion)
- North Korean hackers stole $2 billion in 2025 — no Russia-specific ransomware proceeds estimate available this cycle — Source: Chainalysis
- Russia's A7A5 ruble-backed token processed $93.3 billion in sanctions evasion — Source: Chainalysis 2026 Crypto Crime Report [CREDIBLE REPORTING]

Infrastructure Hosting Patterns

- Media Land LLC (St. Petersburg): Sanctioned by US/UK/Australia in November 2025 (prior reporting period) for supporting LockBit, BlackSuit, Play, BianLian, Lumma Stealer, RedLine, Meduza. Associated entities: ML.Cloud, Aeza Group, Hypercore (UK-registered Aeza front).
- Post-RAMP infrastructure fragmentation: T1erOne emerged as semi-private successor forum; cybercriminal infrastructure migrating away from centralized forums toward distributed, private channels following RAMP seizure
- Specific ASN/provider attribution for April 2026 BPH activity: No reliable data available for this metric in accessible sources this cycle

SECTION 7 — LAW ENFORCEMENT & REGULATORY ACTIONS

New Actions — April 2026

Action 1: OFAC/DOJ Cambodian Scam Center Strike

Lead agency: U.S. Strike Force (DOJ + OFAC coordination); international partners

Date: April 23, 2026

Outcome: 29 OFAC designations; $701.9 million in cryptocurrency restrained; 503 websites seized; multiple Telegram channels seized

Assessed ecosystem impact: Medium — significant financial disruption to Southeast Asian fraud infrastructure; indirect ransomware impact via shared money-laundering networks

Action 2: Europol IOCTA 2026 Publication

Lead agency: Europol

Date: April 28-29, 2026

Outcome: Strategic intelligence publication documenting shift to industrialized cybercrime powered by AI, ransomware, and data theft; 120+ active ransomware brands documented in 2025; confirmed velocity gap between LE and criminal actors widening

Assessed ecosystem impact: Low (direct operational impact); High (informational — confirms structural trends driving legislative and operational prioritization)

Action 3: FBI IC3 2025 Annual Report (Released April 6, 2026)

Lead agency: FBI Internet Crime Complaint Center

Date: April 6, 2026

Outcome: $20.877 billion total cybercrime losses documented; 1M+ complaints received; 63 new ransomware variants identified in 2025; critical infrastructure targeting intensifying

Assessed ecosystem impact: Low (direct); High (policy — first IC3 report to exceed $20B threshold drives congressional and DOJ resource prioritization)

Action 4: Xu Zewei Extradition (HAFNIUM-linked)

Lead agency: U.S. DOJ / Italy (extraditing authority)

Date: April 2026

Outcome: Xu Zewei extradited from Italy to Houston; charged for HAFNIUM-linked intrusions and COVID-19 research targeting (2020-2021); MSS direction and Shanghai Powerock affiliation documented

Assessed ecosystem impact: Low (ransomware ecosystem); Medium (state-nexus intrusion deterrence signaling)

Action 5: Swiss Black Axe Arrests

Lead agency: Swiss cantonal authorities

Date: April 2026

Outcome: 10 suspected Black Axe members arrested across multiple Swiss cantons; alleged Southern Europe regional head detained; cyber-enabled fraud network disrupted

Assessed ecosystem impact: Low (ransomware ecosystem); Medium (BEC/fraud network disruption)

Reconstitution Status Tracker

Operation	Action Date	Target	Action Type	30-Day Status	90-Day Status	180-Day Status
RAMP Seizure (FBI)	Jan 28, 2026	RAMP cybercrime forum	Infrastructure seizure	Partially Reconstituted (T1erOne + fragmented successors within 30 days)	Partially Reconstituted — ecosystem fragmented across multiple smaller forums	Pending (90-day mark: late April 2026)
Media Land / Aeza / Hypercore Sanctions	Nov 19, 2025	Russian BPH infrastructure	OFAC/UK/AU sanctions	Partially Reconstituted — BPH services migrated to non-designated providers	Partially Reconstituted — ~150 days post-action; operations persist under alternative hosting	Pending (180-day: May 2026)
Garantex Redesignation + Grinex Designation	Aug 2025	Garantex / Grinex crypto exchange	OFAC redesignation	Partially Reconstituted — Grinex operated until April 15, 2026 hack	Partially Reconstituted — Grinex suspended April 15; successor channels not yet identified	Pending

Cumulative Impact Assessment — April 2026

Short-term disruption (1-30 days): Low — No major ransomware infrastructure actions occurred in April. Primary April actions targeted fraud/BEC (Cambodia scam centers) and delivered intelligence products (IC3, IOCTA).

Structural ecosystem impact (90+ days): Medium — EU crypto ban (effective May 24) has genuine structural potential to degrade ransomware money-laundering capacity if enforcement holds and non-EU exchanges apply corresponding KYC pressure. RAMP seizure structural impact remains Medium: ecosystem fragmented but not diminished in total volume.

Ecosystem resilience evidence: RAMP reconstituted within 30 days. LockBit (disrupted Feb 2024) returned within 60 days. Media Land sanctions have not visibly reduced total ransomware activity. These data points indicate current enforcement mechanisms produce temporary disruption, not structural degradation. The EU crypto ban represents a qualitatively different financial-layer intervention with longer-duration potential.

SECTION 8 — VULNERABILITY EXPLOITATION MATRIX

Includes CVEs with confirmed exploitation in ransomware/malware campaigns or APT operations during April 2026. Source: CISA KEV catalog updates, The Hacker News, The Register.

CVE	Product	CVSS	Exploitation Method	Threat Actor	Scale/Volume	CISA KEV	KEV Date
CVE-2026-32202	Windows Shell	N/A (zero-day at patch)	Zero-click spoofing via malicious LNK file; victims authenticate attacker server without interaction	APT28 (Fancy Bear / Forest Blizzard)	Targeted — Ukraine and EU nation-states; scale not quantified	Yes	Apr 14, 2026
CVE-2026-21513	Windows (unspecified)	N/A	Exploit chain with CVE-2026-32202; LNK-based delivery	APT28	Same campaign as above	No data	No data
CVE-2026-21643	Fortinet FortiClient EMS	Not confirmed in sources	SQL injection via unauthenticated HTTP requests; enables unauthorized code execution	Unknown (broad exploitation)	Active exploitation observed	Yes	Apr 13, 2026
CVE-2026-34197	Apache ActiveMQ	8.8	Improper input validation; code injection	Unknown threat actors	Active exploitation observed	Yes	Apr 2026
CVE-2026-34621	Adobe Acrobat / Reader	Not confirmed	Prototype pollution vulnerability	Unknown	Active exploitation observed	Yes	Apr 13, 2026
CVE-2023-27351	PaperCut NG/MF	8.2	Improper authentication; unauthenticated access	Multiple ransomware groups (historically)	Active exploitation confirmed	Yes	Apr 2026 re-add
Cisco Catalyst SD-WAN (3 CVEs)	Cisco Catalyst SD-WAN Manager	Multiple	Unspecified; active exploitation confirmed	Unknown	Active exploitation observed	Yes	Late Apr 2026

KEV lag note: CVE-2026-32202 was patched by Microsoft on April 14 without an initial 'exploited in the wild' marking, meaning federal agencies and defenders received no formal urgency signal at patch time. APT28 exploitation was subsequently confirmed and CISA KEV added. This lag between exploitation start and KEV listing — potentially several weeks — represents a structural gap in the current advisory mechanism.

SECTION 9 — SUPPLY CHAIN & THIRD-PARTY COMPROMISE

April 2026 saw a notably high concentration of supply chain attacks affecting developer toolchains and open-source packages. Multiple incidents are attributed to TeamPCP, representing a structured campaign against security and development tooling as an access-sourcing strategy.

Confirmed Supply Chain Incidents — April 2026

Incident 1: Vercel / Context.ai OAuth Breach

Attack chain: Lumma Stealer infection at Context.ai (February 2026) stole Google Workspace OAuth tokens; attackers used tokens to access Vercel internal systems

Disclosed: April 19, 2026 (Vercel CEO public disclosure; Trend Micro analysis)

Compromised component: Context.ai Google Workspace OAuth integration; Vercel internal system access via third-party OAuth

Downstream impact: Vercel user data reportedly offered for sale on BreachForums at $2 million — Source: OX Security. Exact affected environment count: No reliable data available for this metric.

Detection/remediation: Disclosed April 19; Vercel published security bulletin; remediation underway as of late April

Incident 2: Axios npm Package Compromise

Attack chain: Malicious versions axios@1.14.1 and axios@0.30.4 published; injected dependency plain-crypto-js@4.2.1 that downloads multi-stage payloads including a RAT

CISA alert: April 20, 2026

Compromised component: Axios npm package — one of the most widely used JavaScript HTTP libraries

Downstream impact: Potentially millions of dependent projects at risk during exposure window; No reliable count of actively infected environments available

Detection/remediation: CISA alert April 20; Elastic Security Labs analysis published; malicious versions removed from npm

Incident 3: Bitwarden CLI Supply Chain Attack

Attack chain: Malicious version @bitwarden/cli 2026.4.0 published to npm; available for approximately 1.5 hours (5:57 PM to 7:30 PM ET, April 22, 2026)

Attacker: Unknown — Endor Labs analysis published; no attribution confirmed

Compromised component: Bitwarden CLI npm package — credential management tooling for enterprise environments

Downstream impact: Limited by short exposure window (1.5 hours); No reliable data on confirmed infections

Detection/remediation: Identified and removed within 1.5 hours; Endor Labs disclosed

Incident 4: SAP npm Packages — TeamPCP Attribution

Attack chain: Suspicious versions published April 29, 2026 (09:55-12:14 UTC); credential-stealing supply chain attack

Attacker: TeamPCP (attributed by The Hacker News based on TTP overlap with prior TeamPCP operations)

Compromised component: SAP-related npm packages

Downstream impact: No reliable data available for this metric — incident occurred April 29, remediation and scope assessment ongoing

Detection/remediation: Identified same day; The Hacker News reported April 29, 2026

Incident 5: Checkmarx GitHub Actions / Open VSX Plugins (Prior Period, Active Impact)

Attack chain: March 23, 2026: Checkmarx GitHub Actions and Open VSX plugins compromised; part of TeamPCP's structured security-tooling campaign

Attacker: TeamPCP

Downstream impact: Security tooling compromise affecting organizations using Checkmarx CI/CD workflows; scope not publicly quantified

Status: Disclosed; remediated; Checkmarx published advisory

Trend Assessment

- Supply chain attacks as a percentage of total incidents: No reliable data available for this metric. Qualitative assessment: April 2026 represents an anomalously high concentration of confirmed supply chain incidents in a single calendar month — 4 confirmed incidents plus 1 carry-over from March — suggesting either heightened detection awareness or deliberate campaign surge. [ANALYST INFERENCE, medium confidence]
- TeamPCP represents the most operationally significant supply chain threat actor in the reporting period: attributed to at least 3 of the 5 incidents and formally aligned with Vect RaaS as an access-sourcing partner. This is the first documented case of a supply-chain attack group forming a contractual RaaS partnership.

SECTION 10 — ECOSYSTEM CONTROL NODE ANALYSIS

Top Control Nodes Table — April 2026

Rank	Node	Type	Est. Ecosystem Reach	Dependencies	Single Point of Failure?	Disruption Difficulty
1	BreachForums + Vect Integration	Forum / RaaS Platform (hybrid)	300,000+ claimed users; now embedded as ransomware operational infrastructure for Vect affiliate network [CREDIBLE REPORTING]	Internet hosting (distributed); Telegram coordination channels; cryptocurrency payment rails	Partial — forum operator(s) are identifiable choke points; infrastructure is distributed	High — distributed hosting; operator anonymity; prior takedowns of predecessor forums show rapid reconstitution
2	Lumma/Remus Stealer Service	Stealer Service / MaaS	Estimated 40-60% of corporate credential pipeline in 2026 [ANALYST INFERENCE, medium confidence]	C2 infrastructure (now EtherHiding blockchain-based — harder to take down); distribution networks; MaaS subscription infrastructure	Partial — Remus developer identity partially exposed; EtherHiding reduces infrastructure single-point exposure	High — EtherHiding C2 hardens against sinkholing; developer partially doxxed but operational
3	Qilin RaaS Platform	RaaS Platform	Approximately 14% of all tracked ransomware victims in rolling 30-day window [CONFIRMED]	Affiliate recruitment channels; cryptocurrency payment processing; leak site infrastructure	Partial — RaaS platform operator is identifiable choke point; affiliates are distributed	High — operators likely Russia/CIS-based; no identified jurisdiction with realistic extradition exposure
4	Remaining Russian Crypto Exchange Infrastructure (post-Garantex/Grinex)	Crypto Laundry	Ransomware laundering volume: No reliable data available for this metric; structurally critical for monetization [ANALYST INFERENCE]	Russian regulatory tolerance; correspondent banking relationships; OTC broker networks	No — multiple exchanges and OTC brokers provide redundancy	Extreme — Russia-based; beyond Western legal jurisdiction; EU ban (May 24) applies only to EU-nexus transactions
5	TeamPCP Supply Chain Attack Capability	IAB / Supply Chain Attacker	Access sourced to Vect affiliates + independent operations;	npm ecosystem access; open-source toolchain	Partial — group identity may be partially known; TTPs	Medium — operates across developer ecosystems

Rank	Node	Type	Est. Ecosystem Reach	Dependencies	Single Point of Failure?	Disruption Difficulty	
			compromised Checkmarx, Axios, SAP npm, Bitwarden, Telnyx, LiteLLM in 2026 alone [CONFIRMED]	visibility; BreachForums coordination with Vect	are distinctive	without geographic constraints; TTP pattern enables attribution but not apprehension	

Cascade Failure Analysis

Node 1: BreachForums + Vect Integration

- What breaks downstream: Vect's entire affiliate recruitment and key distribution infrastructure. Disruption of BreachForums at this stage — when it has been embedded as operational ransomware infrastructure — would simultaneously eliminate the world's most populated ransomware affiliate pool before it can launch at scale. Secondary: loss of escrow and coordination layer for all forum-dependent criminal transactions.
- Realistic reconstitution timeline: 30-60 days for forum reconstitution based on prior BreachForums seizure history. Vect affiliate keys already distributed cannot be revoked remotely; however, the coordination and leak-site infrastructure would be disrupted. Estimated 60-90 day lag before a functional Vect successor could be operational at comparable scale.
- Enforcement mechanism: DOJ/FBI takedown (prior BreachForums seizure precedent exists); OFAC designation of known operators; hosting provider legal process in non-US jurisdictions where servers are located.

Node 2: Lumma/Remus Stealer Service

- What breaks downstream: Disruption of the primary corporate credential pipeline feeding IAB markets. Without high-volume stealer-derived credentials, IABs face significantly higher costs and lower volume; ransomware groups that rely on credential-based initial access must shift to more expensive and noisier exploit-based entry. The Vercel/Context.ai case illustrates how stealer logs cascade into major enterprise compromises weeks later.
- Realistic reconstitution timeline: Lumma took approximately 2-3 weeks to recover from May 2025 disruption. Remus (already a successor) would require a new replacement cycle; with EtherHiding C2, infrastructure is harder to permanently sinkhole. Estimate: 60-90 days for a functional replacement at scale.
- Enforcement mechanism: Developer identification (partial doxxing already occurred Aug-Oct 2025); financial sanctions on MaaS subscription payment infrastructure; coordinated takedown of C2 infrastructure via blockchain-level interdiction of EtherHiding resolver contracts.

Node 4: Russian Crypto Exchange Infrastructure

- What breaks downstream: Disruption or regulatory closure of the primary ransomware proceeds laundering layer would increase friction costs for all ransomware operators. Grinex suspension (April 15) and EU crypto ban (effective May 24) together represent the first simultaneous pressure on multiple laundering nodes.
- Realistic reconstitution timeline: OTC broker networks can absorb displaced volume within days. A new exchange to replace Garantex/Grinex functionality would require 90-180 days to build trust and liquidity. Displacement to TengriCoin (now EU-sanctioned) and similar Central Asian exchanges is already underway.
- Enforcement mechanism: Secondary sanctions on non-Russian exchanges processing Russian ransomware proceeds (OFAC Section 311 designation); EU's existing May 24 ban; Five Eyes coordinated pressure on Central Asian exchange regulators.

Structural Vulnerability Summary

The most critical structural weakness in the current ecosystem is the monetization layer. The ransomware pipeline is operationally resilient at every other stage — affiliate recruitment is fragmenting into mass-open models, initial access is commoditized, and encryption tooling is widely available. The single most brittle point is conversion of cryptocurrency ransomware proceeds into usable fiat currency through exchange infrastructure that is subject to regulatory action. The EU's May 24 crypto ban, combined with Grinex's April 15 suspension, represents the first credible simultaneous pressure on this layer since the Garantex sanctions in 2022. If enforcement is extended to Central Asian correspondent exchanges and secondary sanctioning is applied to non-compliant VASPs processing Russian ransomware proceeds, monetization friction could reach operationally constraining levels within 90-180 days. No comparable structural vulnerability exists at the access, affiliate, or encryption stages of the current ecosystem.

SECTION 11 — STRATEGIC LEVERAGE ASSESSMENT

Financial Leverage

Leverage Item F-1: EU Crypto Ban Enforcement Window

TARGET: Russian and Belarusian crypto platforms; TengriCoin (Kyrgyz); digital ruble; RUBx stablecoin; OTC brokers displacing Grinex volume

CONDITION: EU 20th sanctions package enacted April 23, 2026; effective May 24, 2026; Grinex suspended April 15, 2026

THRESHOLD: THRESHOLD MET — both trigger conditions are active. Displaced laundering volume will migrate to non-compliant Central Asian and Southeast Asian exchanges within 31 days of May 24 effective date

ACTION: Immediately engage OFAC to designate any exchange absorbing Grinex/Garantex displaced volume under 31 CFR Part 594 (Cyber-Related Sanctions). Simultaneously issue FinCEN Section 311 Special Measures against TengriCoin and any identified Kyrgyz/Central Asian exchange processing Russian ransomware proceeds. Coordinate with Five Eyes counterparts to apply correspondent banking pressure on exchanges without US/EU banking relationships.

WINDOW: 31 days (May 24 effective date). Displaced transaction routing patterns will be observable in blockchain analytics within 2 weeks of May 24; acting before displaced volume consolidates into a new primary exchange is the critical window.

PRIORITY: Critical

Leverage Item F-2: Vect Affiliate Monetization Disruption

TARGET: Vect RaaS cryptocurrency payment processing and negotiation infrastructure; BreachForums escrow services

CONDITION: Vect distributed 300,000+ affiliate keys April 16; VECT 2.0 wiper bug disclosed April 28-29, undermining affiliate confidence and victim willingness to pay; monetization pipeline not yet at scale

THRESHOLD: THRESHOLD MET — Vect is in pre-scale activation phase with structural wiper vulnerability damaging affiliate trust

ACTION: Designate Vect negotiation/payment infrastructure under OFAC Cyber-Related Sanctions before the operation reaches payment scale. Simultaneously, amplify public disclosure of the VECT 2.0 wiper bug to maximize affiliate defection and victim non-payment behavior. Coordinate FBI takedown request for BreachForums infrastructure hosting Vect key distribution and escrow.

WINDOW: 60 days. Vect's wiper bug creates an unusual window where affiliate confidence is structurally undermined; acting before a corrected VECT 3.0 is deployed and trust rebuilds is critical.

PRIORITY: Critical

Infrastructure Leverage

Leverage Item I-1: TeamPCP Attribution and Disruption

TARGET: TeamPCP threat actor group — supply chain access sourcing arm for Vect RaaS

CONDITION: TeamPCP attributed to Checkmarx (March 2026), SAP npm (April 29), and multiple prior supply chain attacks; TTP pattern is distinctive and documented; formal Vect partnership makes them ransomware infrastructure, not merely espionage actor

THRESHOLD: Active — 3 confirmed supply chain attacks in a 40-day window (March 23 to April 29) constitutes an ongoing campaign

ACTION: Escalate TeamPCP to FBI Cyber Division priority designation based on documented Vect RaaS affiliation (ransomware nexus triggers DOJ/FBI jurisdiction). Coordinate with npm security team and GitHub Security Lab for real-time package publication monitoring using TeamPCP TTP signatures. Issue private sector advisory with specific IOCs to npm maintainers and CISA for CI/CD pipeline defenders.

WINDOW: Ongoing — next TeamPCP package publication attempt likely within 30 days based on April campaign tempo

PRIORITY: High

Leverage Item I-2: Remus/LummaC2 C2 Infrastructure Interdiction

TARGET: Remus stealer EtherHiding C2 resolver contracts on Ethereum blockchain; MaaS subscription payment channels

CONDITION: Remus active since February 2026; EtherHiding replaces traditional infrastructure with blockchain-based C2 resolution; developer partially doxxed (Aug-Oct 2025)

THRESHOLD: Active — Remus is scaling as Lumma successor; EtherHiding adoption sets a precedent that will be replicated across other malware families if not interdicted

ACTION: Engage DOJ with Chainanalysis/TRM Labs blockchain forensics to identify and flag EtherHiding resolver contract addresses for interdiction. Coordinate with Ethereum Foundation and major node operators to blacklist identified resolver contracts. Pursue indictment of developers identified during 2025 doxxing campaign to complement infrastructure action.

WINDOW: 90 days — before EtherHiding becomes the dominant C2 evasion technique across the stealer ecosystem

PRIORITY: High

Jurisdictional Leverage

Leverage Item J-1: Central Asian VASP Secondary Sanctions

TARGET: Kyrgyz Republic, Kazakhstan, and UAE-based crypto exchanges absorbing Garantex/Grinex displaced volume

CONDITION: TengriCoin already EU-designated (April 23); Grinex displaced volume will need a new laundering node by May 24

THRESHOLD: THRESHOLD MET — EU designation of TengriCoin confirms displacement has already begun

ACTION: Coordinate OFAC and FinCEN to extend secondary sanctions to any identifiable Kyrgyz, Kazakh, or UAE-based exchange demonstrating absorption of Grinex-displaced volume (observable via blockchain analytics within 2-4 weeks of May 24 effective date). Apply diplomatic pressure through Financial Action Task Force (FATF) to accelerate Kyrgyz Republic grey-listing based on TengriCoin designation.

WINDOW: 45 days — critical window to prevent consolidation of displaced ransomware laundering volume into a single non-sanctioned successor exchange

PRIORITY: High

Coming Month Focus — Top 3 Actions (May 2026)

Priority 1: EU Crypto Ban Enforcement + OFAC Secondary Sanctions Coordination

Expected outcome if action taken: Ransomware laundering friction increases from current estimated 5-10% cost to 20-30% cost as primary exchange displacement routes are closed sequentially. Every incremental exchange designation narrows the viable laundering funnel and raises operational costs for all Russia-linked ransomware operators.

Priority 2: BreachForums / Vect Infrastructure Action During Wiper-Bug Window

Expected outcome if action taken: Disrupting BreachForums while Vect's credibility is structurally damaged by the wiper bug maximizes affiliate defection rate and prevents Vect from reaching operational scale. A combined technical and operational action could reduce the projected affiliate-driven ransomware surge by 30-50% if executed before a corrected VECT 3.0 restores affiliate trust. [ANALYST INFERENCE, medium confidence on impact estimate]

Priority 3: TeamPCP Indictment and CI/CD Pipeline Protection Advisory

Expected outcome if action taken: Public indictment of TeamPCP operators would impose reputational and operational risk on the group's supply-chain access-sourcing model, potentially deterring the Vect-TeamPCP

operational partnership. A CISA advisory with specific TeamPCP IOCs for CI/CD pipeline defenders would reduce the hit rate of future supply chain attacks within the 30-day window while the indictment proceeds.

SECTION 12 — UNCONFIRMED SIGNALS & HORIZON INDICATORS

- Vect mass-activation wave: No confirmed victim surge attributable to the April 16 mass affiliate key distribution has been confirmed in available tracking data as of April 30. [UNCONFIRMED REPORTING] Confirmation indicator: Appearance of Vect-branded victims on leak site at rate exceeding 20/week within 30 days of key distribution. Refutation indicator: Continued absence of Vect leak-site posts by May 16 would suggest affiliate activation rate is low despite key distribution.

- VECT 3.0 corrected release: Security researchers noted the wiper bug in VECT 2.0 on April 28-29. A corrected version with functional encryption is likely in development. [ANALYST INFERENCE, medium confidence] Confirmation indicator: New Vect version announcement on BreachForums or dark web forums within 30-60 days. Refutation indicator: Vect leadership silence or shutdown messaging would indicate the project is abandoned.

- Post-RAMP forum consolidation around T1erOne: Early intelligence suggests T1erOne is positioning as the primary RAMP successor for Russian-language ransomware coordination. [UNCONFIRMED REPORTING] Confirmation indicator: Documented IAB listings and affiliate recruitment posts migrating to T1erOne with volume comparable to former RAMP activity. Refutation indicator: Multiple competing forums each achieving partial RAMP-like functionality without a single dominant successor.

- A7A5 stablecoin resilience to EU ban: Russia's ruble-backed A7A5 token ($93.3B estimated sanctions evasion volume) may be insulated from EU crypto ban by operating primarily outside EU-nexus transactions. [ANALYST INFERENCE, medium confidence] Confirmation indicator: Post-May 24 blockchain analysis showing A7A5 transaction volume unchanged or increased. Refutation indicator: EU enforcement actions targeting specific A7A5 liquidity providers with EU banking relationships.

- The Gentlemen rebranding or transition: The SystemBC C2 exposure on April 21 revealed the group's true operational scale to researchers. Groups historically rebrand following significant infrastructure exposure. [ANALYST INFERENCE, low confidence] Confirmation indicator: The Gentlemen leak site goes dark within 60 days and a new group with similar TTPs (SystemBC, GPO abuse, Cobalt Strike) appears. Refutation indicator: The Gentlemen continues posting at normal cadence with no operational changes.

SECTION 13 — ANALYTIC CAVEATS & COLLECTION GAPS

Sources Blocked During Collection

- ransomware.live — Not fetched; network access restricted (not on allowlist). Monthly victim totals sourced from secondary reporting (Breachsense, ReliaQuest, ZeroFox) that cite ransomware.live as primary source.
- ransomlook.io — Not fetched; network access restricted. Q1 2026 ransomlook.io figure (2,570 incidents) sourced from ReliaQuest secondary citation.
- ransom-db.com — Not fetched; network access restricted. April 2026 group-level victim data sourced from search result excerpts from ransom-db weekly reports.
- bleepingcomputer.com, therecord.media, mandiant.com, secureworks.com, crowdstrike.com, shadowserver.org, ic3.gov, chainalysis.com (direct fetch), trmlabs.com (direct fetch) — All blocked. Intelligence sourced via web search result summaries and secondary citations where available.

Data Unavailable or Unreliable This Cycle

- April 2026 final victim count: Reporting period ends April 30; final monthly total not yet compiled by tracking platforms. Figures used are partial/rolling.
- Sector-by-sector prior-month comparatives: Not available in accessible sources; Sector Targeting Trend Table prior month column populated with 'No prior data' per Rule 2.
- Time-to-publish (leak site signal): No reliable metric available from accessible sources; gap noted in Three-Signal Composite per Rule 2.
- Encryption-free extortion as percentage of total incidents: Qualitative trend confirmed (Europol IOCTA, ReliaQuest); specific percentage unavailable per Rule 2.
- IAB market listing volume (current): No reliable monthly count available post-RAMP seizure; RAMP was the primary tracked forum; successor forums not yet generating comparable observable data.
- Ransomware aggregate proceeds estimate: No reliable monthly figure available; FBI IC3 full-year 2025 figure cited as closest available benchmark.
- Vect victim count: Affiliate activation too recent (April 16) for reliable victim tracking in accessible sources as of April 30.

Sections Omitted

No sections were fully omitted this cycle; all required sections contained sufficient confirmed or credible data to meet the Rule 1 threshold. The Leak Site Time-to-Publish signal (Section 2) and several financial metrics carry explicit 'No reliable data available' notations per Rule 2.

Known Inflation/Deflation Biases

- Victim count inflation: Groups post victims who paid ransoms to pressure non-payers; some victims appear on multiple group sites; negotiation victims are sometimes posted after payment as retaliation. All victim counts are therefore potentially inflated relative to actual confirmed incidents.
- Victim count deflation (more significant): The Gentlemen C2 analysis (1,570 actual vs. 320 published) demonstrates that leak-site counts undercount actual operational reach by a factor of 3-5x. Published counts represent only victims who refused to pay or were selected for public pressure — not total operational victims.
- Financial figures: Ransom payment figures are self-reported or derived from blockchain analytics with known coverage gaps. Dark Web OTC transactions may not be captured in Chainalysis/TRM Labs figures.

Competing Explanations for Major Trends

- Ecosystem fragmentation vs. expansion: The record 91 active leak sites in Q1 2026 can be interpreted as (a) ecosystem growth driven by lower barriers to entry, or (b) artificial inflation as single operators run multiple small sites for operational security. Both explanations may be simultaneously true.
- Vect threat level: The mass BreachForums affiliate partnership could indicate (a) a genuinely novel threat requiring immediate action, or (b) a marketing exercise that overstates Vect's actual operational capability given the wiper bug and likely low real-world affiliate conversion rate from 300,000 nominally registered forum members.
- EU crypto ban impact: The ban could (a) meaningfully degrade ransomware monetization by closing the most accessible laundering channels, or (b) produce minimal impact if Russian operators have already migrated to non-EU-nexus exchanges and OTC brokers that are beyond EU regulatory reach. Both scenarios are plausible; impact will be observable in on-chain data post-May 24.

SOURCES

Ransomware Tracking Platforms

- Ransomware.live — https://www.ransomware.live (not directly fetched; cited in secondary sources)
- Ransomlook.io — https://www.ransomlook.io (not directly fetched)
- Breachsense — March 2026 Ransomware Report: https://www.breachsense.com/ransomware-reports/march-2026/
- Ransom-DB — April 2026 Threat Landscape: https://www.ransom-db.com/blog/ransomware-threat-landscape-report-april-2026

Government and Law Enforcement

- CISA Known Exploited Vulnerabilities Catalog — https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- CISA Alert — Axios npm Supply Chain Compromise — https://www.cisa.gov/news-events/alerts/2026/04/20/supply-chain-compromise-impacts-axios-node-package-manager
- FBI IC3 2025 Annual Report — https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf
- OFAC — Cambodia Scam Center Designations — https://home.treasury.gov/news/press-releases/sb0225
- OFAC — Media Land / Aeza Sanctions — https://home.treasury.gov/news/press-releases/sb0319
- EU Council — 20th Russia Sanctions Package — https://www.consilium.europa.eu/en/press/press-releases/2026/04/23/russia-s-war-of-aggression-against-ukraine-20th-round-of-stern-eu-sanctions-hits-energy-military-industrial-complex-trade-and-financial-services-including-crypto/
- Europol IOCTA 2026 — https://www.europol.europa.eu/publication-events/main-reports/iocta-2026-evolving-threat-landscape

Vendor Threat Intelligence

- Check Point Research — The Gentlemen / SystemBC DFIR Report — https://research.checkpoint.com/2026/dfir-report-the-gentlemen/
- Check Point Research — VECT Ransomware by Design — https://research.checkpoint.com/2026/vect-ransomware-by-design-wiper-by-accident/
- Trend Micro — Vercel OAuth Supply Chain Attack — https://www.trendmicro.com/en_us/research/26/d/vercel-breach-oauth-supply-chain.html
- Elastic Security Labs — Axios RAT Analysis — https://www.elastic.co/security-labs/axios-one-rat-to-rule-them-all
- Endor Labs — Bitwarden CLI Supply Chain — https://www.endorlabs.com/learn/shai-hulud-the-third-coming
- Gen Digital — Remus / Lumma Successor — https://www.gendigital.com/blog/insights/research/remus-64bit-variant-of-lumma-stealer
- Dataminr — Vect / BreachForums / TeamPCP — https://www.dataminr.com/resources/intel-brief/vect-breachforums-teampcp-converge-in-unprecedented-affiliate-mobilizatio/
- Cynet — Vect RaaS Affiliate Playbook — https://www.cynet.com/blog/how-vect-ransomware-is-rewriting-the-raas-affiliate-playbook/

Cybersecurity News

- The Hacker News — SystemBC / The Gentlemen: https://thehackernews.com/2026/04/systembc-c2-server-reveals-1570-victims.html
- The Hacker News — CVE-2026-32202 Windows Shell: https://thehackernews.com/2026/04/microsoft-confirms-active-exploitation.html
- The Hacker News — CISA KEV Fortinet/Microsoft/Adobe: https://thehackernews.com/2026/04/cisa-adds-6-known-exploited-flaws-in.html

- The Hacker News — VECT 2.0 Wiper: https://thehackernews.com/2026/04/vect-20-ransomware-irreversibly.html
- The Hacker News — SAP npm / TeamPCP: https://thehackernews.com/2026/04/sap-npm-packages-compromised-by-mini.html
- The Hacker News — Apache ActiveMQ KEV: https://thehackernews.com/2026/04/apache-activemq-cve-2026-34197-added-to.html
- The Register — CVE-2026-32202 Zero-Click: https://www.theregister.com/2026/04/29/microsoft_zero_click_exploit/
- The Register — Vect Wiper Bug: https://www.theregister.com/2026/04/28/dont_pay_vect_a_ransom/
- The Register — Supply Chain Ongoing Campaign: https://www.theregister.com/2026/04/27/supply_chain_campaign_targets_security/
- Infosecurity Magazine — The Gentlemen Expansion: https://www.infosecurity-magazine.com/news/gentlemen-ransomware-rapid/
- CoinDesk — EU 20th Sanctions Crypto: https://www.coindesk.com/policy/2026/04/27/eu-s-largest-measures-against-russia-yet-include-escalation-of-crypto-sanctions-evasion

Financial Intelligence

- Chainalysis — Southeast Asia Scam Centers / Crypto April 2026: https://www.chainalysis.com/blog/asian-scam-centers-crypto-fraud-april-2026/
- Chainalysis — EU 20th Sanctions Package Analysis: https://www.chainalysis.com/blog/eu-russia-sactions-package-april-2026/
- Chainalysis — 2026 Crypto Sanctions Overview: https://www.chainalysis.com/blog/crypto-sanctions-2026/
- Breached.Company — Grinex Hack $13.7M: https://breached.company/grinex-crypto-exchange-hack-13-million-russia-sanctions-2026/
- TRM Labs — 2026 Crypto Crime Report: https://www.trmlabs.com/reports-and-whitepapers/2026-crypto-crime-report

Analytical Reports and Surveys

- ReliaQuest — Q1 2026 Ransomware and Cyber Extortion: https://reliaquest.com/blog/threat-spotlight-ransomware-and-cyber-extortion-in-q1-2026/
- ZeroFox — Q1 2026 Ransomware Wrap-Up: https://www.zerofox.com/intelligence/q1-2026-ransomware-wrap-up/
- Emsisoft — State of Ransomware Q1 2026: https://www.emsisoft.com/en/blog/47562/the-state-of-ransomware-in-q1-2026/
- Security Affairs — RAMP Uncovered: https://securityaffairs.com/191171/cyber-crime/ramp-uncovered-anatomy-of-russias-ransomware-marketplace.html
- Industrial Cyber — IOCTA 2026 Report: https://industrialcyber.co/reports/europol-iocta-2026-report-flags-shift-to-industrialised-cybercrime-powered-by-ai-ransomware-and-data-theft/
- Industrial Cyber — FBI IC3 Critical Infrastructure: https://industrialcyber.co/reports/fbi-reports-cyber-threats-to-critical-infrastructure-intensify-as-us-cybercrime-losses-hit-21-billion-exposes-risk/
- Morphisec — Ransomware Without Encryption: https://www.morphisec.com/blog/ransomware-without-encryption-why-pure-exfiltration-attacks-are-surging-and-why-theyre-so-hard-to-catch/
- Nerds.xyz — Q1 2026 Ransomware: https://nerds.xyz/2026/04/ransomware-q1-2026/