MONTHLY CYBERCRIME ECOSYSTEM INTELLIGENCE REPORT

Coverage Period: June 2026

Classification: ANALYST USE

Produced by: EDP Intelligence Cell

Date: July 1, 2026

Confidence labels used throughout: CONFIRMED / CREDIBLE REPORTING / ANALYST INFERENCE. Every URL cited was retrieved via web fetch during collection (Rule 5); sources that failed retrieval are listed in Section 13.

SECTION 1 — EXECUTIVE SUMMARY

Five items, priority ranked by ecosystem-level strategic impact. Each carries a supporting metric and a confidence label.

1. Operation Endgame's June 15 to 24 strike on the loader and stealer supply chain (StealC, Amadey, SocGholish) actioned 326 servers and 142 domains, recovered 27 million stolen credentials, and restricted roughly 41 million euros in crypto, hitting the credential-supply layer that feeds ransomware affiliates rather than end-stage payloads. *CONFIRMED.*
2. June leak-site volume rose to approximately 722 organizations (BreachSense live index) from 646 in May, a provisional increase near 12 percent that reverses the prior two months of decline, with Qilin assessed as the dominant operator for a sixth consecutive month. *CREDIBLE REPORTING / ANALYST INFERENCE.*
3. OFAC's June 2 designation of four Iranian crypto exchanges (Nobitex alone represents roughly 50 percent of Iranian digital-asset inflows) plus a June 22 ISIS-facilitator action mark the largest US action to date against Iran's digital-asset sector and extend exchange-level financial chokepoints as a primary lever. *CONFIRMED.*
4. Encryption-free data extortion consolidated as a dominant model, with World Leaks, ShinyHunters (Oracle PeopleSoft zero-day, 100-plus organizations), and Silent Ransom Group (roughly 100 listed victims) all operating pure-exfiltration in June; the best available baseline is 22 percent of incident-response cases running data-only, up roughly elevenfold year over year. *CREDIBLE REPORTING.*
5. A SaaS OAuth-abuse supply-chain compromise (Klue to Salesforce, 14-plus named downstream enterprises) plus a confirmed CIS-exclusion enforcement event (the Nova crew banned an affiliate for hitting Uzbek and Moscow-linked oilfield firm Eriell) confirm both the accelerating SaaS-vendor vector and continued Russian safe-harbor self-policing. *CREDIBLE REPORTING.*

SECTION 2 — RANSOMWARE ECOSYSTEM: MONTHLY STATISTICS

Total victims disclosed (June 2026): approximately 722 organizations posted to leak sites (BreachSense live June index). This is a still-accruing tracker count; no finalized month-end analytical report was published as of July 1. CREDIBLE REPORTING.

Prior month baseline (May 2026): 646 victims, 61 active groups, 73 countries, 59 industries (BreachSense May report). CONFIRMED per source.

Month-over-month change: approximately +12 percent (722 vs 646), computed across two same-methodology BreachSense figures. ANALYST INFERENCE, provisional, given June is still accruing.

Active group count (2026 YTD): 106 active groups across 130 countries; 4,780 victims YTD through July 1 (ransomware.live). A June-only active-group count is not reliably available.

New groups identified (2026 YTD): 37 tracked new groups. June debuts include Black X (Jun 2), Triple X (Jun 13), Deadlock (Jun 15), Wallstreet (Jun 26), Settra (Jun 28, 22 victims rapidly), Redact (Jun 28), and Blackfield (Jun 29, demanded 2M USD from Nidec). CREDIBLE REPORTING (ransomware.live / BleepingComputer).

Defunct or dormant groups: No reliable June-specific attrition count available. Structural context: The Record reports roughly 50 new groups appear and roughly 30 exit per year; top-10 concentration has fallen to about 50 percent of attacks from 69 percent in 2022.

Estimated ransom volume: No reliable data available for June. Annual context: the 2025 ransom-paid rate fell to 28 percent (Chainalysis, cited via Securelist).

Sector Targeting Trend Table

June finalized sector-level breakdown was not published as of July 1. The table reflects the most recent complete finalized month (May 2026) versus April 2026, preserving a quantitative backbone. Source: BreachSense monthly reports.

Sector	May 2026 (n)	April 2026 (n)	% Change	Trend
Manufacturing	58	50	+16%	Increasing
Healthcare	54	64	-16%	Decreasing
Construction	42	37	+14%	Increasing
Consumer Goods	38	37	+3%	Stable
Finance	31	28	+11%	Increasing
Technology	31	56	-45%	Decreasing

Geographic Targeting Analysis

- Countries hit more frequently: The United States remains the dominant target at 39.3 percent of May victims (254 of 646); UK 36, Canada 31, Germany 29, Spain 21. No finalized June geographic breakdown is available. CREDIBLE REPORTING.
- CIS-exclusion holding: A confirmed enforcement event occurred in early June. The Nova crew (an affiliate program of the RAlord operation) banned an affiliate for hitting Eriell Group, an oilfield-services firm headquartered in Uzbekistan with Moscow offices, then issued a public apology, pledged no leak, and offered free recovery. This is textbook safe-harbor self-policing to avoid creating domestic victims who trigger Russian law enforcement. *CREDIBLE REPORTING.*
- Targeting divergence: The Gentlemen is a notable outlier, with only about 13 percent of victims US-based (Thailand, UK, Brazil, Germany, India lead), diverging from the ecosystem's typical US-heavy distribution. *CREDIBLE REPORTING (The Hacker News).*

Leak Site Three-Signal Composite

Signal	This Month (June)	Prior Month (May)	Trend	Notes
Post Volume (victims published)	~722 (provisional)	646	Increasing ~+12%	Source: BreachSense / ransomware.live
Time-to-Publish (avg days, compromise to publication)	No reliable data	No reliable data	N/A	Collection gap persists; extortion-only actors (SRG) compress

Signal	This Month (June)	Prior Month (May)	Trend	Notes
				to under one business day
Takedown/Relaunch Cycle (days dark to successor)	RAMP ~150 days dark; LeakBase ~90 days not reconstituted	RAMP ~120 days dark	Lengthening	Longer cycle = higher resilience cost imposed

Composite interpretation: Post volume is rising while time-to-publish remains an unresolved collection gap, so we cannot confirm whether groups are publishing more victims faster or simply publishing more. The lengthening takedown-to-relaunch cycle (RAMP now anomalously dark past 150 days, versus a typical 60-to-90-day gap) is the most analytically significant signal: it indicates enforcement is imposing durable reconstitution cost on the forum layer even as the RaaS victim count climbs. ANALYST INFERENCE, medium confidence.

SECTION 3 — THREAT ACTOR LANDSCAPE

Russia and CIS-linked groups prioritized. Victim counts are cumulative or most-recent-finalized where June actuals are unavailable.

Qilin

- Victim count (June): no reliable standalone figure; leak feed saturation on June 30 and 546 cumulative victims YTD through May indicate continued dominance.
- Key development: assessed to hold the number-one operator position for a sixth consecutive month; formal BreachForums partnership persists. CREDIBLE REPORTING / ANALYST INFERENCE.
- Threat level shift: Stable (elevated). CIS-exclusion: Assessed (Russian-speaking, Russia-based per The Record).

The Gentlemen (aka Phantom Mantis / Storm-2697)

- Victim count: 478 cumulative (The Hacker News, Jun 11); about 483 across 66 countries by mid-June.
- Key development: operator publicly identified as Alexander Andreevich Yapaev of Izhevsk, Russia (Brian Krebs); Go-based, Garble-obfuscated locker with self-propagating worm capability and an anti-recovery wipe routine; 90/10 affiliate split; heavy AI use in development. CREDIBLE REPORTING.
- Threat level shift: Increasing. CIS-exclusion: Assessed (Russian-speaking operator, Izhevsk-based).

INC Ransomware (and Lynx / Sinobi lineage)

- Victim count: 830-plus cumulative since August 2023, 65-plus percent US; 4th in Q1 2026 (120-plus incidents, ZeroFox).
- Key development: Windows and Linux/ESXi encryptors rewritten in Rust; code-overlapping families Lynx and Sinobi spun off after a May 2024 source-code sale. CONFIRMED reporting.
- Threat level shift: Stable. CIS-exclusion: Assessed.

World Leaks (rebrand of Hunters International)

- Victim count (June flagship): Tata Electronics, an Apple iPhone contract manufacturer, with 204,341 files / 630.4 GB listed June 12; confirmed by BleepingComputer June 23.
- Key development: operates purely as data extortion with no encryption, following the July 2025 wind-down of Hunters International. CONFIRMED.
- Threat level shift: Increasing. CIS-exclusion: Assessed.

Nova (RAlord affiliate program)

- Victim count: 23 in May; a June affiliate ban is the notable event rather than a volume figure.
- Key development: enforced its CIS-exclusion rule in early June by banning an affiliate who hit Eriell Group and publicly apologizing. CREDIBLE REPORTING.
- Threat level shift: Stable. CIS-exclusion: Confirmed (actively enforced).

Silent Ransom Group / UNC3753 (Luna Moth, Conti offshoot)

- Victim count: roughly 100 victims listed as of June across LEAKEDDATA and a business-data-leaks domain.
- Key development: end-to-end extortion within one business day using vishing plus in-person USB theft; leak infrastructure runs on an 18-country, 22-ISP residential botnet to resist takedown. CONFIRMED (Mandiant / Resecurity).
- Threat level shift: Increasing. CIS-exclusion: Assessed (Conti lineage, Russian-language).

Data Extortion Trend

- Current share of encryption-free extortion: best available baseline is 22 percent of Arctic Wolf incident-response cases running data-only. The primary source failed retrieval, so treat as CREDIBLE REPORTING, not confirmed. No verified June-specific percentage is available.
- Named extortion-only groups active in June: World Leaks, ShinyHunters (UNC6240), Silent Ransom Group (UNC3753), and Clop. CONFIRMED via multiple June articles.
- Month-over-month change: No reliable data. Year-over-year context: an approximately elevenfold rise (2 percent to 22 percent of IR cases) over the prior twelve months. CREDIBLE REPORTING.

SECTION 4 — INITIAL ACCESS & TTP EVOLUTION

Access-vector ranking below uses the most recent complete incident-response dataset (Cisco Talos IR Trends, Q1 2026), as no net-new June ranking was published. Source: Talos.

6. Phishing: reclaimed the number-one initial-access position, appearing in over one third of engagements, after the ToolShell/SharePoint exploitation wave subsided.
7. Valid accounts: 24 percent of engagements.
8. Exploitation of public-facing applications: 18 percent, down sharply from 62 percent as ToolShell activity declined.

TTP developments (June-specific):

- ClickFix as-a-service evolution (published June 30): payloads are now generated on demand by API servers that wrap each request in rotating encryption (Base64/AES/TripleDES/Rijndael/Deflate) over a shared in-memory PowerShell core, with 25-language lures and macOS plus Windows targeting. A new Downloads-folder AMSI-evasion method keeps malicious code out of the clipboard. ClickFix accounted for 47 percent of Microsoft Defender Experts initial-access cases and now carries MITRE ATT&CK ID T1204.004. CONFIRMED / CREDIBLE REPORTING.

- Execution drift: actors moved from the Win+R Run box to Win+X / Windows Terminal to avoid leaving RunMRU forensic artifacts; top launchers are PowerShell and cmd (about 39 percent each) and msiexec (about 34 percent). CREDIBLE REPORTING.
- First documented adversarial use of a named AI web-builder (Softr, vibe coding) to construct a phishing and credential-harvest page in a Talos IR case. CONFIRMED.

IAB Market Indicators Table

No net-new June IAB market report was published; the authoritative dataset remains Rapid7 H2 2025 (published March 31, 2026). Figures below are explicitly dated and used as the best-available baseline.

Indicator	This Period (H2 2025, latest)	Prior Period	Trend
Volume of corporate access listings	DarkForums 221 + RAMP 208 threads = 81% of observed IAB threads	Lower; more dispersed	Consolidating
Median access price	RAMP representative ~$6,400; overall avg base $113,275 (skewed by DarkForums)	~$2,726 avg base	Increasing
Premium listing ceiling	Tied to avg alleged victim revenue $3.242B	Lower	Increasing (up-market shift)
Most-targeted sectors (top 3)	Government 14.2%, Retail 13.1%, IT 10.8%	Comparable	Stable
Dominant access type	RDP 21.2%, then VPN 12.8%, RDWeb 11.2% (Citrix behind RDP/VPN on RAMP)	RDP-led	Stable
Notable marketplace events	IntelBroker (Kai West) arrest cut BreachForums IAB threads ~52% YoY; Oracle EBS CVE-2025-61882 exploit offered on RAMP	-	Enforcement pressure

SECTION 5 — MALWARE & STEALER ECOSYSTEM

Families ranked by June relevance and observed distribution. The defining June event was the Operation Endgame phase targeting the loader and stealer front end of the ransomware supply chain.

StealC

- Version 2.2.1 as of June; sold at $300/month by actor plymouth; top infections in the US, Poland, Italy. Distributed via Amadey, MintsLoader, and ClickFix/FileFix. Disruption status: core infrastructure actioned in Operation Endgame (June 15 to 24). CONFIRMED.

Amadey

- Version 5.87; 11,635 samples distributed in 2025 (peak), 1,837 YTD 2026; its largest botnet cluster delivered Lumma, Vidar, StealC, RedLine, SmokeLoader, XWorm, AsyncRAT, and Rhadamanthys across 53 clusters. Disruption status: actioned in Operation Endgame. CONFIRMED.

SocGholish (Evil Corp-linked)

- Fake-browser-update injection into compromised WordPress; 14,971 infected WordPress sites remediated during the June operation. Disruption status: disrupted alongside StealC and Amadey. CONFIRMED.

LummaC2

- Resurfaced within days of its May 2025 takedown (which disrupted over 2,300 domains) and reportedly leads 2026 distribution alongside StealC and Vidar per AhnLab trend data. The primary source could not be fully retrieved, so 2026 market-share ranking is CREDIBLE REPORTING, not confirmed. No confirmed 2026 infection-volume figure obtained.

RedLine

- Referenced only as a legacy, declining family whose logs still circulate post-Operation Magnus (October 2024). No change. CREDIBLE REPORTING.

Infostealer-to-IAB Pipeline

- Constella processed 51.7 million infostealer packages in 2025 (up 72 percent YoY) across 24.8 million unique infected devices. CONFIRMED per source.
- 78 percent of recently breached organizations had corporate credentials in infostealer logs within the six months before the breach (Constella); Verizon 2025 DBIR reports 54 percent of ransomware victims had domain credentials in stealer-log marketplaces before attack. CONFIRMED (secondary citation for DBIR).
- Timing: the widely repeated sub-48-hour infection-to-sale window is CREDIBLE REPORTING only; the fetched primary reframes 48 hours as an exposure-to-exploitation response window, not a measured interval. Freshness commands a premium because session tokens expire, and session cookies (which bypass MFA with no login event) are the most operationally dangerous artifact.

SECTION 6 — FINANCIAL & INFRASTRUCTURE SIGNALS

Sanctions & Enforcement Actions

Authority	Target	Rationale	Est. Exposure	Impact
OFAC (Jun 2)	Nobitex, Wallex, Bitpin, Ramzinex + 4 Nobitex execs	Sanctions evasion, terror financing, IRGC-linked ransomware facilitation	Nobitex ~50% of Iranian inflows; ecosystem >$7.78B in 2025	High
OFAC (Jun 22)	3 individuals + 6 entities (Bitcoin Xchange, Spider, Alkaram, 3 Nigerian bureaux); 2 TRON wallets	ISIS financial facilitation	Not quantified per source	Medium

Financial-flow observations (dollar figures from named sources):

- AudiA6 laundering service: approximately 336 million euros laundered since 2021; 692,000 euros frozen plus 86,000 euros seized; 393.39 BTC (about 19.2 million USD) traced from illicit sources within roughly 10,333 BTC deposited. CONFIRMED (DOJ / The Hacker News).
- Operation Endgame (June phase): approximately 41 million euros in crypto frozen. CONFIRMED (Europol / Infosecurity Magazine).
- Iran campaign: roughly 500 million USD in regime-linked crypto frozen (Chainalysis/OFAC, CONFIRMED); a Treasury figure of roughly 1 billion USD total recovered attributed to Secretary Bessent is CREDIBLE REPORTING, not independently verified.
- 2025 US context: over 20 billion USD in online-fraud losses (up 26 percent YoY); about 11.36 billion USD in crypto-scam losses (FBI, via BeInCrypto). CONFIRMED per source.

Infrastructure Hosting Patterns

- Sanctioned Stark Industries / PQ Hosting reportedly rebranded in June to THE.Hosting under WorkTitans B.V., migrating from AS44477 to AS209847 to evade EU sanctions after a May 18 Dutch seizure of 800-plus servers. The primary June source failed retrieval, so the ASN and WorkTitans detail is CREDIBLE REPORTING, not verified. See Section 12.
- Prior context (out of window): the November 2025 US/AU/UK sanctions on Media Land (St. Petersburg BPH), ML Cloud, and the Aeza/Hypercore rebrand chain remain the baseline for Russian BPH reconstitution behavior. CONFIRMED but dated November 2025.

SECTION 7 — LAW ENFORCEMENT & REGULATORY ACTIONS

New Actions This Month

- FBI Operation Riptide (announced June 9 to 10): a 60-day, whole-of-FBI campaign across all 56 field offices implementing Executive Order 14390; search warrants, indictments, worldwide arrests, and millions in crypto seized to date; named target First VPN (alleged to have serviced 25-plus ransomware groups). Assessed ecosystem impact: Medium, because dollar and arrest totals were undisclosed and much of the effort is a strategic umbrella over discrete actions. CONFIRMED (BeInCrypto).
- AudiA6 takedown (June 10): Europol, US Secret Service, and IRS-CI with 10 countries; 2 administrators arrested in Georgia; DOJ charged Ruslan Igorevich Tkachuk (37) and Alexander Vladimirovich Ledenev (25); 25 domains, 30-plus servers, and 80-plus vehicles seized, and the linked Dark2Web forum taken down. Assessed impact: Medium-High, dismantling a laundering service tied to 15-plus ransomware and crypto-theft investigations. CONFIRMED (The Hacker News).
- Operation Endgame, new chapter (June 15 to 24): Europol, Germany's BKA, and the Netherlands with Microsoft DCU and industry partners dismantled StealC, Amadey, and SocGholish infrastructure; 326 servers and 142 domains actioned, 27 million credentials recovered, over 200 C2 servers disrupted, and 18,000-plus victim computers identified. Assessed impact: High, targeting a core credential-supply layer. CONFIRMED (Europol / Security Affairs).
- OFAC designations (June 2 and June 22): detailed in Section 6. Assessed impact: High (Iran exchanges) and Medium (ISIS facilitators).

Reconstitution Status Tracker

Prior-cycle actions updated at 30/90/180-day intervals; June actions added at initiation. Status options: Fully / Partially / Not Reconstituted / Pending / No Data.

Operation	Action Date	Target	Action Type	30-Day	90-Day	180-Day
RAMP Forum Seizure	Jan 28, 2026	RAMP forum	Seized	Dark	Dark (anomalous)	Not Reconstituted (~150d; 180-day due Jul 28)
LeakBase Seizure	Mar 2026	LeakBase	Seized	Not Reconstituted	Not Reconstituted (~90d)	Pending
BKA REvil ID	Apr 6, 2026	REvil/GandCrab ops	Warrants	No arrest	No arrest (~85d)	Pending
Operation Saffron	May 19-20, 2026	1vpns anonymization	33 servers seized	Not Reconstituted (~40d)	Pending	Pending
Stark / Dutch FIOD	May 18-27, 2026	Stark BPH	~800 servers seized	Partially Reconstituted (THE.Hosting/ WorkTitans AS209847, CREDIBLE)	Pending	Pending
Lumma Stealer LE	May 2025	Lumma C2 (2,300 domains)	Seized	Past	Past	Fully Reconstituted
Operation Endgame (StealC/Amadey)	Jun 15-24, 2026	Stealer/loader infra	326 servers	Pending (~2 wks)	Pending	Pending
AudiA6 Takedown	Jun 10, 2026	Laundering service	Seized	Pending (~3 wks)	Pending	Pending

Cumulative Impact Assessment

Short-term disruption (1 to 30 days): High. The June actions removed operational infrastructure across three ecosystem layers simultaneously: stealer/loader supply (Operation Endgame), laundering (AudiA6), and exchange-level cashout (OFAC Iran). The 27 million recovered credentials and 41 million euros frozen represent immediate, measurable removal of criminal capacity.

Structural ecosystem impact (90-plus days): Medium. Reconstitution history tempers the structural score. Lumma fully reconstituted within weeks of its 2025 takedown and is now assessed to lead 2026 distribution; the Stark BPH network appears to have rebranded (WorkTitans/AS209847) within roughly a month of seizure. The RAMP forum is the lone durable exception, dark past 150 days versus a typical 60-to-90-day gap, suggesting that forum-layer disruption imposes more lasting cost than stealer-infrastructure seizure when developers remain at large. ANALYST INFERENCE, medium confidence.

SECTION 8 — VULNERABILITY EXPLOITATION MATRIX

CVEs with confirmed exploitation in ransomware or malware campaigns during June, cross-referenced against CISA KEV. Note: all cisa.gov fetches returned empty bodies (Section 13); KEV facts are corroborated via Rapid7, The Hacker News, and BleepingComputer.

CVE	Product	CVSS	Method / Actor	Scale	KEV / Date
CVE-2026-50751	Check Point VPN	9.3	IKEv1 auth bypass, then ELF payload; Qilin affiliate (medium/high conf.)	Several dozen orgs; spike early June	Yes; Jun 8-9
CVE-2026-33825 (BlueHammer)	MS Defender (Win LPE)	High	SAM DB access to SYSTEM; unnamed ransomware gangs	Not quantified	Yes; added Apr 22, ransomware-flagged Jun 30
CVE-2026-35273	Oracle PeopleSoft	Critical	Zero-day data theft (no encryption); ShinyHunters	300+ instances / 100+ orgs	Not confirmed in KEV
CVE-2026-20245	Cisco Catalyst SD-WAN Mgr	7.8	Command exec as root; not attributed	Not quantified	Yes; Jun 9
CVE-2026-11645	Google Chrome V8	8.8	OOB read/write RCE; not attributed	Not quantified	Yes; Jun 9
CVE-2026-7473	Arista EOS	6.9	Improper tunnel decapsulation; not attributed	7020/7280/7500R series	Yes; Jun 9

Only CVE-2026-50751 (Check Point / Qilin) and CVE-2026-33825 (BlueHammer) meet the strict criterion of confirmed exploitation in ransomware campaigns during June. CVE-2026-35273 is confirmed exploitation in a data-theft extortion campaign. The Cisco, Chrome, and Arista entries are confirmed actively exploited and KEV-listed but not tied to a named ransomware operator in retrieved sources. Notable lag: BlueHammer was KEV-listed April 22 but only flagged as ransomware-exploited June 30, an approximately 69-day gap between listing and confirmed ransomware use.

SECTION 9 — SUPPLY CHAIN & THIRD-PARTY COMPROMISE

Klue to Salesforce OAuth Abuse (SaaS supply chain)

- Attacker Icarus (active since April 28) compromised a disused-but-active legacy Klue integration credential around June 11 to 12, pivoted into Klue infrastructure, harvested customer OAuth tokens, and queried downstream Salesforce CRMs at scale (roughly 1,000 automated queries per 15-minute burst). Salesforce disabled the Klue Battlecards integration.

- Confirmed downstream victims: Huntress (3.4 GB leaked), Jamf, Recorded Future, Tanium, Gong, HackerOne, Snyk, LastPass, BeyondTrust, OneTrust, Sprout Social, Pendo, Insurity, and 8x8. ReliaQuest linked the TTPs to the 2025 Salesloft Drift / Gainsight OAuth-abuse playbook. Remediation: tokens and credentials revoked, integration disabled. CONFIRMED (The Hacker News).

Atomic Arch (Arch Linux AUR hijack, open-source supply chain)

- From around June 11, attackers adopted 400-plus orphaned AUR packages, spoofed git commit metadata, and edited install scripts to deliver a Rust credential stealer (deps) with an optional eBPF rootkit and systemd persistence. Tracked by Sonatype as Sonatype-2026-003775 (CVSS 8.7); no CVE assigned; official Arch repos unaffected. Remediation: maintainers resetting commits and banning accounts. CONFIRMED.

Oracle PeopleSoft Zero-Day (third-party enterprise software)

- ShinyHunters exploited CVE-2026-35273 for data theft across 300-plus instances and 100-plus organizations (education-heavy), with Nissan disclosing an employee-data breach June 29. Oracle issued emergency mitigations; Mandiant confirmed exploitation May 27 to June 9. CONFIRMED (BleepingComputer).

Trend Assessment

- Supply chain as a percentage of total incidents: No reliable verified June figure available. Search-surfaced figures (297 supply-chain attacks in 2025, up 93 percent) could not be retrieved from source and are excluded. What is verifiable is a qualitative acceleration of the SaaS-vendor-as-vector pattern, with ReliaQuest and Obsidian explicitly linking June's Klue compromise to the 2025 Salesloft Drift wave. Obsidian (verified quote): compromising one vendor means access to hundreds of enterprise environments at once. CREDIBLE REPORTING.

SECTION 10 — ECOSYSTEM CONTROL NODE ANALYSIS

Top Control Nodes Table

Rank	Node	Type	Est. Ecosystem Reach	SPOF?	Disruption Difficulty
1	Stablecoin cashout (USDT)	Crypto Laundry	95% of illicit inflows to sanctioned entities transit stablecoins; $93B sanctioned flows 2025 (est., med conf.)	Partial (Tether chokepoint)	Extreme
2	Qilin RaaS	RaaS Platform	~21% of Q1 2026 victims; dominant 6th month (est., high conf.)	Partial	High
3	Infostealer-to-IAB pipeline	IAB Market	54% of ransomware victims had creds in stealer markets pre-attack; 51.7M packages 2025	No	Extreme
4	DarkForums + RAMP	Forum / IAB Market	81% of observed IAB threads H2 2025 (est., med conf.)	Partial	High
5	LummaC2 / StealC MaaS	Stealer Service	Leading 2026 distribution; drives credential-to-IAB pipeline (est., med conf.)	Partial	High
6	The Gentlemen RaaS	RaaS Platform	~15% of 2026 YTD victims; operator identity now public	Partial	Medium-Low
7	First VPN /	BPH / Other	Serviced 25+ ransomware	Yes (per FBI	Medium

Rank	Node	Type	Est. Ecosystem Reach	SPOF?	Disruption Difficulty
	anonymization layer		groups (FBI Riptide target)	framing)	

Cascade Failure Analysis

Stablecoin cashout (USDT): If removed, the payment-collection chain for the majority of Russian and CIS ransomware operations breaks, because roughly 95 percent of illicit inflows to sanctioned entities transit stablecoins and alternatives remain immature at the required scale. Realistic reconstitution timeline: long (12-plus months) if the pressure targets the issuer rather than individual wallets. Enforcement mechanism: regulatory action against Tether and correspondent-banking access, not wallet-by-wallet sanctions.

Infostealer-to-IAB pipeline: If removed, ransomware affiliates lose the fresh corporate-credential feed behind at least 54 percent of victims. But the node is decentralized across hundreds of Telegram channels and MaaS families and reconstitutes within weeks, as Lumma demonstrated. Enforcement mechanism: sustained, repeated coordinated takedowns on the Operation Endgame model rather than a single strike.

Qilin RaaS: If removed, roughly one fifth of monthly victim volume is displaced, but affiliates migrate to competing platforms within weeks and the operator identity is not public. Enforcement mechanism: none currently effective, as no jurisdiction with enforcement authority has acted against a Russia-nexus operator.

Structural Vulnerability Summary

The single most critical structural weakness is the stablecoin cashout chokepoint. Every otherwise-decentralized layer of the ecosystem (RaaS platforms, IAB markets, stealer services, bulletproof hosting) shares one hard dependency: converting extorted funds into usable value, and roughly 95 percent of that flow moves through USDT. Unlike forums or stealer infrastructure, which reconstitute in weeks, a credible regulatory action against the dominant stablecoin issuer has no near-term substitute at scale. The ecosystem is most brittle at the point where crypto meets the regulated financial system, and least brittle at the RaaS and IAB layers, which are built for rapid rebranding and migration.

SECTION 11 — STRATEGIC LEVERAGE ASSESSMENT

Financial Pressure

TARGET: Dominant stablecoin issuer (Tether/USDT) and correspondent-banking access.

CONDITION: Roughly 95 percent of illicit inflows to sanctioned entities transit stablecoins; $93B in sanctioned flows in 2025.

THRESHOLD: THRESHOLD MET. Sanctioned-entity stablecoin dependence is already documented above the actionable line.

ACTION: Designate specific issuer-adjacent intermediaries and correspondent accounts servicing sanctioned Russian and Iranian flows, replicating the June 2 Iranian-exchange model against the cashout layer.

WINDOW: Open now; narrows as alternative laundering rails (A7A5 and non-custodial chains) mature over the next 2 to 4 quarters.

PRIORITY: Critical.

Infrastructure Pressure

TARGET: Stark / PQ Hosting successor THE.Hosting under WorkTitans B.V. (AS209847).

CONDITION: Reported June rebrand and ASN migration (AS44477 to AS209847) within roughly a month of the May Dutch seizure indicates active reconstitution.

THRESHOLD: Confirm the AS209847/WorkTitans linkage (currently CREDIBLE, primary source blocked); linkage confirmation is the trigger.

ACTION: Sanction WorkTitans B.V. and de-peer AS209847 through upstream providers, applying the Dutch sanctions-law theory established against Stark.

WINDOW: 30 to 60 days before the successor network re-establishes stable peering and customer migration completes.

PRIORITY: High.

Infrastructure Pressure (Stealer Reconstitution)

TARGET: Lumma / StealC reconstituted hosting following the June Operation Endgame seizure.

CONDITION: Lumma fully reconstituted after its 2025 takedown; StealC and Amadey developers remain at large post-June seizure.

THRESHOLD: First confirmed StealC/Amadey C2 re-emergence on new infrastructure post-June 24.

ACTION: Pre-stage a second Endgame-model strike on successor C2, coordinated with hosting-provider de-peering, rather than treating the June action as terminal.

WINDOW: The 3-to-6-month reconstitution window observed in prior stealer takedowns.

PRIORITY: High.

Jurisdictional Pressure

TARGET: The Gentlemen operator Alexander Andreevich Yapaev (Izhevsk, Russia).

CONDITION: Operator identity and affiliate TOX IDs publicly exposed; group at number-two YTD position and Increasing.

THRESHOLD: THRESHOLD MET. Identity exposure is the trigger and it has occurred.

ACTION: Issue indictment and Interpol Red Notice, seize identified affiliate infrastructure, and pursue third-country arrest opportunities while the operator's operational security is degraded.

WINDOW: 60 to 90 days before the operator hardens OPSEC and rebrands, per the Embargo-to-ArmCorp-to-Gentlemen precedent.

PRIORITY: High.

Coming Month Focus (Top 3)

9. Pre-stage a second Operation Endgame strike on StealC/Amadey/Lumma successor infrastructure. Expected outcome: convert a one-time seizure into sustained denial, preventing the weeks-scale reconstitution seen after the 2025 Lumma action.
10. Confirm and act on the WorkTitans/AS209847 linkage. Expected outcome: sanction and de-peer the Stark successor before customer migration completes, denying 25-plus ransomware-adjacent tenants stable hosting.

11. Indict and Red-Notice The Gentlemen operator while identity exposure is fresh. Expected outcome: force OPSEC hardening and rebranding costs on the number-two RaaS operator, degrading affiliate confidence during the exposure window.

SECTION 12 — UNCONFIRMED SIGNALS & HORIZON INDICATORS

- **[UNCONFIRMED REPORTING]** Stark/PQ Hosting rebranded to THE.Hosting under WorkTitans B.V. with migration to AS209847. Primary source (BankInfoSecurity) was gated. Confirm via: independent ASN/WHOIS attribution linking AS209847 to WorkTitans and to prior Stark tenants.
- **[UNCONFIRMED REPORTING]** Roughly 1 billion USD in Iranian crypto recovered (attributed to Treasury Secretary Bessent). Confirm via: a primary Treasury press release with the figure.
- **[UNCONFIRMED REPORTING]** LummaC2 leads 2026 stealer distribution (AhnLab trend data). Confirm via: a fully retrievable AhnLab or Trend Micro quarterly with 2026 market-share percentages.
- **[UNCONFIRMED REPORTING]** INTERPOL Operation First Light 2026 with 276 arrests and 701 million USD seized. This appears to fall earlier in 2026, not within June; excluded from Section 7. Confirm via: an INTERPOL primary release with dates.
- **[ANALYST INFERENCE]** The June leak-site volume uptick (+12 percent provisional) may reflect deferred publication from May rather than a genuine rise in compromises. Refute via: finalized June sector and time-to-publish data showing whether victim intake or publication cadence drove the increase.
- **[ANALYST INFERENCE]** Early-warning for July: expect StealC/Amadey C2 re-emergence within 30 to 60 days (per prior stealer reconstitution timelines) and continued SaaS OAuth-abuse compromises following the Klue and 2025 Salesloft Drift pattern. Confirm via: new C2 telemetry and additional Salesforce/OAuth downstream disclosures.

SECTION 13 — ANALYTIC CAVEATS & COLLECTION GAPS

Sources Blocked During Collection (Step 1.5 verification)

- cisa.gov (KEV catalog and June 9/23/25 alert pages): all fetches returned empty bodies (bot/CDN blocking). KEV facts corroborated via Rapid7, The Hacker News, BleepingComputer.
- europol.europa.eu/media-press/newsroom (and the AudiA6 press page): JavaScript single-page app; body did not render. Corroborated via The Hacker News and Infosecurity Magazine.
- ofac.treasury.gov/recent-actions: not in provenance set; could not be fetched. Press-release numbers corroborated via Chainalysis.
- bankinfosecurity.com (Lumma resurgence; sanctioned-host DNS-hijacking): registration/JS wall; only headline and meta retrievable. The Stark/WorkTitans/AS209847 detail therefore remains unverified.
- therecord.media (StealC/Amadey/SocGholish takedown article): fetch returned empty body.
- microsoft.com/en-us/security/blog (June 24 StealC/Amadey post): response exceeded tool token limit; figures corroborated via verified secondary sources.
- hipaajournal.com (elevenfold data-only extortion increase): empty body. The 22 percent / 11x Arctic Wolf figure is therefore CREDIBLE REPORTING, not verified.
- theregister.com (Nova/Eriell primary): not in provenance set. Corroborated via Ciphers Security.
- sharkstriker.com (June breaches, 701 figure): fetched, but the 701 figure was not present in the body; BreachSense 722 used instead.
- deepstrike.io (supply-chain statistics): exceeded fetch size limit; trend percentages excluded.

Data Unavailable or Unreliable This Cycle

- No finalized June-2026 monthly analytical report was published as of July 1; the 722 total is a live, still-accruing tracker count and the +12 percent MoM is a provisional computation.
- June-specific sector, geography, and ransom-volume breakdowns are unavailable; May 2026 finalized data is used as the baseline throughout Section 2.
- Time-to-publish (compromise-to-publication) remains an unresolved collection gap, limiting the leak-site composite interpretation.
- IAB market metrics derive from Rapid7 H2 2025 (published March 2026), not fresh June telemetry; presented as the best-available, explicitly dated baseline.

Analytic Notes and Biases

- Securelist/Kaspersky is a Russian-origin vendor; its figures are weighted accordingly.
- Leak-site victim counts inflate reality (they include unverified claims and exclude victims who pay quietly) and can also deflate it (groups that never publish). The 722 count is a lower bound on activity, not a census.
- Competing explanation for the June volume uptick: deferred May publication versus genuine growth in compromises; unresolved pending finalized data. Competing explanation for lengthening takedown cycles: durable enforcement cost versus voluntary operator dormancy to evade heat.

Sections Omitted

- No sections were omitted. All required standing sections met the Rule 1 data threshold, with explicit no-reliable-data notations where June-specific figures were unavailable.

SOURCES

Ransomware Tracking Platforms

1. ransomware.live — 2026 statistics
2. ransomware.live — all-time and new-groups
3. BreachSense — May 2026 ransomware report
4. BreachSense — June 2026 breaches index
5. Check Point Research — State of Ransomware Q1 2026
6. Securelist (Kaspersky) — State of Ransomware 2026

Government & Law Enforcement

7. BeInCrypto — FBI Operation Riptide
8. The Hacker News — Europol disrupts AudiA6
9. Infosecurity Magazine — Operation Endgame StealC/Amadey
10. Security Affairs — Operation Endgame StealC/Amadey

Vendor Threat Intelligence

11. Rapid7 — IAB shift to high-value targets (H2 2025)
12. Rapid7 — Check Point VPN zero-day CVE-2026-50751
13. Cisco Talos — IR Trends Q1 2026
14. Constella — infostealer-to-breach pipeline

Cybersecurity News

15. The Hacker News — The Gentlemen ransomware profile
16. The Hacker News — INC ransomware profile
17. The Hacker News — UNC3753 vishing/physical extortion

18. The Hacker News — Amadey and StealC takedown
19. The Hacker News — ClickFix API-driven payloads
20. The Hacker News — CISA adds Cisco/Chrome/Arista flaws
21. The Hacker News — Klue/Salesforce OAuth supply chain
22. The Hacker News — Atomic Arch AUR supply chain
23. The Hacker News — FortiBleed FortiGate campaign
24. BleepingComputer — Tata Electronics / World Leaks
25. BleepingComputer — BlueHammer now exploited by ransomware
26. BleepingComputer — Nissan / Oracle PeopleSoft zero-day
27. The Record — ransomware takedowns and proliferation
28. Ciphers Security — Nova/Eriell CIS-rule enforcement

Financial Intelligence

29. Chainalysis — OFAC sanctions Iranian crypto exchanges
30. Chainalysis — OFAC sanctions ISIS financial facilitators

Infrastructure Intelligence

31. Security Affairs — coordinated BPH sanctions (Nov 2025, context)