EDP INTELLIGENCE CELL

MONTHLY CYBERCRIME ECOSYSTEM INTELLIGENCE REPORT

Coverage Period: MAY 2026

Classification: ANALYST USE

Produced by: EDP Intelligence Cell

Report Date: 31 May 2026

Sources: Ransomware.live, Breachsense, Check Point Research, Rapid7, Chainalysis, TRM Labs, Flare, Verizon DBIR, CISA KEV

SECTION 1 — EXECUTIVE SUMMARY

Five items, priority ranked by ecosystem-level strategic impact. All items confirmed. Each includes a supporting metric.

Priority	Finding	Confidence
1 — HIGHEST IMPACT	Operation Saffron (May 19-20) and the Dutch FIOD Stark Industries seizure (~May 18-27) simultaneously removed First VPN — anonymization infrastructure used by 25 ransomware groups — and 800 bulletproof servers hosting Russian-nexus attack and disinformation operations, the most coordinated infrastructure strike against the ecosystem since Operation Cronos.	CONFIRMED
2	The Gentlemen RaaS — the ecosystem's second most active operator with approximately 332 YTD victims — suffered an internal backend breach on May 4 that exposed admin identity zeta88/hastalamuerte, 8 affiliate TOX IDs, 29 campaign samples, the full cash-out chain (Tinkoff QR codes, OTC delivery), and a confirmed $190,000 ransom payment; law enforcement has a narrow 30-60 day window before operational security rebuilds.	CONFIRMED
3	Ransomware's payment model is structurally collapsing: 69% of victims refused payment in 2025 (Verizon 2026 DBIR), ransom payment rates have fallen from 76% (2019) to 28% (2026, Kaspersky), and 95% of illicit ransomware proceeds now transit stablecoin infrastructure — principally USDT via the $72B A7A5 token cluster — creating a single, targetable financial chokepoint.	CONFIRMED
4	CVE-2026-20182 (Cisco Catalyst SD-WAN Controller, CVSS 10.0) was added to CISA KEV on May 14-15 after active exploitation by at least 10 distinct threat clusters including UAT-8616 since March 2026, representing a ~70-day gap between initial exploitation and federal advisory that exposed unpatched organizations throughout the period.	CONFIRMED
5	The ransomware ecosystem has reconsolidated after 2025 fragmentation: Qilin, The Gentlemen, Akira, and LockBit 5.0 collectively accounted for 41% of Q1 2026 victims (2,122 total), while the top 10 groups controlled 71% — a cartel-level concentration reversing the prior quarter's fragmentation and making targeted action against the top-4 platform operators the highest-leverage disruption strategy available.	CONFIRMED

SECTION 2 — RANSOMWARE ECOSYSTEM: MAY 2026 STATISTICS

2.1 Monthly Volume & Active Groups

- Total victims, April 2026 (confirmed): 772 — Source: Breachsense April 2026 Report
- Total victims, May 2026 (tracking estimate as of late May): approximately 700, representing a 9.4% month-over-month decline — Source: Ransomware.live. Final count will update at month close.
- YTD 2026 total (through late May): approximately 3,894 across 97 active groups and 119 countries — Source: Ransomware.live
- Q1 2026 total (Jan-Mar confirmed): 2,122 victims — Source: Check Point Research State of Ransomware Q1 2026 (May 11, 2026). This is 12.2% below the Q4 2025 all-time record of 2,416 but the second-highest Q1 on record.
- 2026 on-pace annual projection: approximately 8,800 victims based on YTD run rate — a ~20% increase over 2025's confirmed 7,307.
- Active groups in 2026: 97 — Source: Ransomware.live
- New groups debuted in May 2026 (through late May): 8 — Fulcrumsec (23 victims), Leakbazaar (9), Blackwater (6), Cmdorganization (4), Prinzeugen (1), Icarus (1), Shadowbyt3$ (reactivated), Titan. Combined May victim count: 61.
- Estimated ransom volume — FY 2025 total on-chain ransomware payments: $820 million (8% YoY decline from $892 million in 2024). Median payment: $59,556 (up 368% from $12,738 in 2024), indicating a shift to fewer but larger payments. No May 2026 monthly aggregate available — No reliable data available for this specific metric. Source: Chainalysis 2026 Crypto Crime Report.

2.2 Sector Targeting Trend (April 2026 vs. March 2026)

Source: Breachsense April 2026 Report. April actuals; March provided for comparison.

Sector	April 2026 (n)	March 2026 (n)	% Change	Trend / Notes
Healthcare	64	47	+36%	Increasing — leading critical-sector target
Technology	56	36	+56%	Increasing — fastest-growing April sector
Manufacturing	50	76	-34%	Decreasing — monthly volatility; remains YTD leader
Legal Services	40	43	-7%	Stable
Consumer Goods	37	28	+32%	Increasing
Construction	37	53	-30%	Decreasing
IT Services	31	35	-11%	Stable
Education	30	26	+15%	Increasing
Engineering	29	No prior data	N/A	New in April top 10; no March baseline available

Sector	April 2026 (n)	March 2026 (n)	% Change	Trend / Notes
Finance	28	48	-42%	Decreasing — record median demand ($3M) despite lower count

2.3 Geographic Targeting Analysis

Source: Breachsense April 2026 Report.

Rank	Country	Victims (Apr)	% of Total	Notes vs. March
1	**United States**	304	39.4%	-10.6 pts (was 50% in March) — absolute targeting unchanged; geographic spread widening
2	**Germany**	37	4.8%	+0.6 pts
3	**United Kingdom**	34	4.4%	+1.3 pts
4	**Canada**	28	3.6%	+1.4 pts
5	**France**	27	3.5%	-1.2 pts
6	**Italy**	26	3.4%	+0.4 pts
7	**Spain**	21	2.7%	+0.4 pts
8	**Australia**	19	2.5%	Stable
9	**India**	16	2.1%	+0.3 pts
10	**Thailand**	16	2.1%	New in April top 10 — Southeast Asia expansion signal

- CIS-exclusion assessment: The CIS-exclusion norm has fractured among newer entrants. Qilin, The Gentlemen, and DragonForce show no consistent CIS-exclusion policy. No Russia/CIS victims attributed to these groups appeared in April or May tracking data, but this is assessed as opportunistic rather than policy-driven. LockBit 5.0 resumed operations without publishing a CIS-exclusion policy. Assessed CIS-exclusion weakening among non-legacy groups — ANALYST INFERENCE, medium confidence.
- SORM and deliberate non-enforcement — CONFIRMED CAPABILITY: Russia's SORM (System of Operative Investigative Measures) architecture requires all Russian ISPs and telecoms to install FSB-controlled intercept hardware ('black boxes') providing the FSB unmediated, real-time access to all communications traffic on Russian IP infrastructure — without ISP visibility into what is being collected. This is established technical and legal fact, documented in Russian federal law and confirmed by multiple Western intelligence assessments. Its analytical implication for this report: the FSB's technical visibility into Russian-IP ransomware operator behavior is categorical, not probabilistic. Russian authorities can observe operator communications, financial flows, and infrastructure in real time. 'Deliberate non-enforcement' of ransomware groups operating on Russian infrastructure is therefore not a capability gap — it is a confirmed policy choice made by an actor with full technical visibility. This upgrades the evidentiary basis of the non-enforcement inference from 'medium confidence' to 'high confidence' on the capability component, while the policy intent component remains ANALYST INFERENCE, high confidence.

- Thailand's entry into the April top-10 (tied 9th, 16 victims) is the clearest geographic expansion signal this cycle — Southeast Asia is emerging as a secondary growth market for ransomware targeting, consistent with The Gentlemen's confirmed Thailand presence in verified reporting.
- The U.S. share drop from 50% to 39.4% in April reflects geographic spread (79 countries hit in April vs. 75 in March), not reduced U.S. targeting. U.S. absolute victim count declined from 385 to 304 in April, consistent with overall volume decline.

2.4 Leak Site Three-Signal Composite

Signal	This Month	Prior Month	Trend	Notes
Post Volume (victims published)	~700 est. May; 772 confirmed April	772 (April)	Down ~9.4% MoM	Breachsense April 2026 Report; May tracking estimate from Ransomware.live
Takedown/Relaunch Cycle	RAMP: seized Jan 28; no confirmed successor at 120+ days (anomalous — typical 60-90 day reconstitution)	RAMP active (pre-Jan)	Resilience cost HIGH	120+ day absence is longest observed gap since RAMP launch in 2021

Composite interpretation: Post volume is trending down ~9.4% MoM, consistent with — though not exclusively attributable to — the Operation Saffron / Stark Industries infrastructure disruptions and the RAMP forum void. The RAMP 120+ day non-reconstitution is the single most anomalous structural signal this cycle; typical gap is 60-90 days. Time-to-publish data remains a collection gap. The volume decline combined with an unknown time-to-publish trajectory means we cannot confirm whether groups are publishing fewer victims or simply slower — analytically significant for ransom leverage assessment.

SECTION 3 — THREAT ACTOR LANDSCAPE

Russia/CIS-linked groups prioritized. Victim counts are April 2026 actuals from Breachsense April 2026 Report except where noted. Q1 counts from Check Point Research.

Group	Victims (Apr / Period)	Cumul. Proceeds	Key May Development	Threat Level	CIS-Excl.
Qilin	103 (Apr); 445 YTD	No reliable data	Led victim disclosures 4th consecutive month; formal BreachForums partnership (300,000+ users) announced March 2026; 26 confirmed healthcare victims YTD (17% of all healthcare DLS listings)	Stable — dominant tier	Unknown (no published CIS-exclusion policy)
The Gentlemen	82 (Apr); ~332 YTD	No reliable data	May 4 backend breach exposed admin identity zeta88/hastalamuerte, 8 affiliate TOX IDs, full cash-out chain, $190,000 confirmed payment, CVE tracking list — unprecedented intelligence windfall	Increasing — then disrupted	Unknown
DragonForce	63 (Apr); growing every month in 2026	No reliable data	Consistent monthly growth (Feb 30 → Mar 54 → Apr 63); on trajectory to challenge Qilin volume by Q3 2026 if trend continues — ANALYST INFERENCE; shared infrastructure overlap with LockBit and Qilin confirmed	Increasing	Unknown
Akira	48 (Apr); volatile (Jan 71, Feb 39, Mar 84, Apr 48)	No reliable data	VPN exploitation confirmed as dominant access vector: S-RM 2026 reports VPN devices account for 68% of remote-access exploit cases, with nearly 70% of those linked to Akira campaigns; BYOVD attacks confirmed	Stable — high volatility	Assessed (historically observed)
LockBit 5.0	39 (Apr); 163 Q1 2026	No reliable data	Comeback confirmed by Check Point (+106% vs Q4 2025); May 9 claimed VP Brands International (Bulgaria); cross-platform (Windows/Linux/ESXi); climbed from outside top 10 to 4th globally in Q1	Increasing — comeback trajectory confirmed	Assessed (historically observed)
INC Ransom	41 (Apr)	No reliable data	Consistent top-5 operator; targets US, Canada, Germany, Australia, UK; sectors include professional services, healthcare, government, manufacturing — Source: Cyfirma May 2026	Stable	Unknown

Group	Victims (Apr / Period)	Cumul. Proceeds	Key May Development	Threat Level	CIS-Excl.
WorldLeaks (Hunters Intl. rebrand)	13 (Apr); 31 since Jan 2026 relaunch	No reliable data	Encryption-free exfiltration model since January 1 2025 relaunch; targeted American Battery Factory in May; embodies the pure-extortion trend; represents a complete operational pivot from traditional RaaS	Stable — pioneering the dominant 2026 attack model	Unknown
Payload	~50 total since Feb 2026 launch	No reliable data	Babuk-derived source code; cross-platform (Windows + ESXi); targets healthcare, energy, real estate, agriculture; claimed 12 victims in 7 countries within hours of launching	Increasing — new entrant, rapid accumulation	Unknown
Karakurt	Inactive (legacy)	$56M+ from 54+ victims ($15M confirmed paid)	May 6: negotiator Deniss Zolotarjovs (Latvian, 35) sentenced to 8.5 years; DOJ confirmed gang used Russian government database access and paid military draft bribes — establishing state-facilitation precedent	Decreasing — legacy, leadership sentenced	Confirmed (leadership sanctioned)

3.2 The Gentlemen — Operational Intelligence Deep-Dive (May 4, 2026)

Source: Check Point Research 'Thus Spoke...The Gentlemen' (May 13, 2026) — verified source. The May 4 internal backend breach of The Gentlemen's Rocket database is the most significant actor-specific intelligence event of the reporting period.

- **Admin Identity:** zeta88 / hastalamuerte — manages RaaS platform, builds the locker, runs payouts, AND directly conducts infections. TOX ID: F8E24C7F5B12CD69C44C73F438F65E9BF560ADF35EBBDF92CF9A9B84079F8F04060FF98D098E. Admin built the GLOCKER panel in 3 days using AI-assisted coding; prefers DeepSeek, Qwen, and Kimi models.
- **Affiliate Structure:** 8 distinct affiliate TOX IDs identified across 29 confirmed campaigns. Most active affiliate (TOX 98C132E2...) ran 11 of 29 campaigns. 90/10 split model (90% to affiliate). ~9 named operators in leaked communications.
- **Cash-out chain (CONFIRMED):** BTC → exchange chains via ~800 'buy desk' transactions → Tinkoff bank QR code cash-out (minimum 400,000 rubles / ~$4,400 USD per transaction) → OTC physical cash delivery. Non-custodial wallets (Guarda, Trust Wallet, Exodus) used to avoid KYC/AML at centralized exchanges.
- **Confirmed payment:** $190,000 USD received (initial ask $250,000) in one documented negotiation. Admin drafts tailored follow-up letters citing GDPR exposure, regulatory risk, and reputational damage to maximize payment pressure.
- **CVEs actively tracked:** CVE-2024-55591 (FortiOS), CVE-2025-32433 (Erlang SSH/Cisco — PoC shared in TOOLS channel and actively evaluated), CVE-2025-33073 (NTLM relay — integrated into

RelayKing for systematic scanning). All three beyond typical threat intel tracking — the group evaluates PoC reliability before operational deployment.

- **Novel dual-leverage tactic:** Data stolen from a UK software consultancy was reused to attack a Turkish company. The UK firm was then publicly attributed as the 'access broker' on the DLS, pressuring the Turkish victim to pursue legal action against the UK victim — a cascading extortion chain multiplying pressure without additional intrusion cost.
- **Infrastructure breach origin:** Likely 4VPS hosting provider compromise. Admin immediately acknowledged the leak on underground forums May 4 and announced infrastructure overhaul: new NAS, restructured communications, updated locker (hardware breakpoint removal, NTDLL unhooking, ETW patching).
- **Full breach dataset size:** A screenshot shared on an underground forum shows a total leak size of approximately 16.22 GB — confirmed in the Check Point Research report (May 13, 2026). Check Point Research obtained and analyzed a partial 44.4 MB subset. The full 16.22 GB dataset likely contains complete victim records, negotiation logs, payment wallet history, and affiliate communications beyond what was analyzed in the partial leak. If this full dataset is in law enforcement or researcher hands, it would represent a near-complete operational record of the group since its mid-2025 founding.

3.3 Data Extortion Trend (Encryption-Free)

- Encryption-free extortion share: Kaspersky State of Ransomware 2026 (May 11) characterizes pure data extortion as the 'default playbook' as of 2026 but does not publish a specific percentage. A figure of approximately 35% for Q1 2026 appears in vendor reporting (Morphisec, Cybersecurity Insiders) but is not confirmed in a primary verified source — treat as CREDIBLE REPORTING, low-to-medium confidence. The more robustly sourced indicators are directional: ransom payment rates have collapsed from 76% (2019) to 28% (2026, Kaspersky); 69% of victims refused payment in 2025 (Verizon 2026 DBIR). These figures confirm the encryption leverage thesis is failing, which structurally drives the extortion-only shift regardless of the precise percentage. Competing explanation in Section 13.4: pre-encryption extortion pressure may be misclassified as encryption-free in some vendor datasets.
- Named groups confirmed operating extortion-only: WorldLeaks (Hunters International), ShinyHunters, Cl0p (Oracle zero-day campaign — see Section 8). DentaQuest listed by ShinyHunters in May using pure exfiltration model.
- Structural driver: Encryption-free is faster, harder to detect (no mass file modification signature), avoids decryptor operational complexity, and remains fully effective for payment pressure via regulatory and reputational threat. Backups provide zero protection against the extortion component, which now applies to an estimated one-third or more of attacks.

SECTION 4 — INITIAL ACCESS & TTP EVOLUTION

4.1 Access Vector Ranking (May 2026)

Ranked most to least common. Sources: Rapid7 H2 2025 IAB Report, S-RM 2026 Cyber Incident Insights, Check Point Research Gentlemen leak analysis.

- 1. RDP (Remote Desktop Protocol) — 21.2% of IAB listings (Rapid7 H2 2025). Direct exposure hardening is pushing attackers toward RDWeb portals (11.2% of listings, up from near-zero in prior periods).
- 2. VPN Exploitation — 12.8% of IAB listings but 68% of actual remote-access exploit cases handled by S-RM in 2026, with nearly 70% linked to Akira campaigns. FortiGate and Cisco SD-WAN are confirmed primary targets (CVE-2024-55591, CVE-2026-20182 — see Section 8).
- 3. RDWeb (Remote Desktop Web Access) — 11.2% of IAB listings; growing as direct RDP exposure declines.
- 4. Phishing / Infostealer-derived credential abuse — IBM X-Force: 84% YoY increase in infostealers delivered via phishing (2024 data). The Gentlemen's OWA/M365 credential log ('ЛБ logs') channel demonstrates direct stealer-to-RaaS pipeline with no IAB intermediary, compressing attack chain further.
- 5. Vulnerability exploitation of public-facing applications — CISA KEV additions accelerating (12 vulnerabilities added in a single April 2026 week). CVE-2026-20182 exploited by 10+ clusters; Oracle CVE-2025-61882 (CVSS 10.0) sold as zero-day on RAMP by Cl0p actor.
- 6. Supply chain / CI/CD compromise — Mini Shai-Hulud (May 10-11) and DAEMON Tools compromise (April-May) demonstrate software supply chain as a scaled access vector. See Section 9.

4.2 Significant TTP Developments This Cycle

- **BYOVD EDR Killing:** Qilin and Akira both confirmed using Bring Your Own Vulnerable Driver attacks to disable EDR before encryption. The Gentlemen's TOOLS channel systematically distributes EDR killer kits (EDRStartupHinder, gfreeze, glinker). 54 EDR killers exploiting 35 signed vulnerable drivers documented across the broader 2026 ecosystem.
- **AI-Assisted Development:** The Gentlemen admin built the GLOCKER RaaS panel in 3 days using AI coding assistance. Prefers DeepSeek, Qwen, and Kimi over Western LLMs. Operators discussing self-hosted uncensored LLMs for automated triage of exfiltrated victim data — not yet implemented but actively planned. First documented case of Chinese LLMs being operationally preferred in RaaS development.
- **Dual-Leverage Extortion Chains:** Documented in The Gentlemen case: stolen data from Victim A reused in attack on Victim B, then Victim A publicly attributed as the 'access broker' to pressure Victim B into legal action against Victim A — cascading extortion at zero additional intrusion cost.
- **CI/CD OIDC Token Extraction:** Mini Shai-Hulud demonstrated pull_request_target misconfiguration enables extraction of OIDC tokens from CI runner memory, producing malicious

packages with valid SLSA provenance — bypassing software supply chain integrity controls deployed post-SolarWinds.

4.3 IAB Market Indicators

Note: H2 2025 $113,275 average is heavily skewed by DarkForums' premium listings; Rapid7 expanded sampling to include DarkForums and RAMP for the first time in H2 2025. Forum-normalized price comparison would show a more moderate increase. This report accepts the Rapid7 methodology while flagging the confound.

Indicator	This Period (H2 2025-May 2026)	Prior Period	Trend
Volume of corporate access listings	~530 observed threads across 5 forums in H2 2025 (Rapid7)	~400 observed threads (Rapid7 2025 Report)	Increasing
Average IAB base price	$113,275 H2 2025 average (Rapid7); NOTE: DarkForums' premium listings heavily skew this average — forum-normalized price shows more moderate increase	$2,726 (FY 2024, Rapid7)	+4,055% — partially a sampling expansion artifact
Premium listing ceiling	>$100,000	>$100,000	Stable
Most-targeted sectors (top 3)	Government 14.2%, Retail 13.1%, IT 10.8% (Rapid7 H2 2025)	Financial Services, IT (prior periods)	Government now dominant — shift from financial services
Dominant access type (listings)	RDP 21.2%, VPN 12.8%, RDWeb 11.2% (Rapid7 H2 2025); VPN devices = 68% of actual exploit cases handled by S-RM	VPN 45%, RDP 41% (prior period)	RDP now leads listings; VPN leads exploitation cases
Notable marketplace events	RAMP seized Jan 28, 2026 (120+ days dark); BreachForums 323,986-user DB exposed; DarkForums grew 600% Apr-Jun 2025; Vect-BreachForums partnership Mar 2026	BreachForums repeated seizures 2023-24	Ecosystem migrating to DarkForums and private channels

SECTION 5 — MALWARE & STEALER ECOSYSTEM

Sources: AhnLab ASEC Feb 2026, Flare 2026 State of Enterprise Infostealer Exposure (May 25, 2026), Recorded Future, TrendMicro, SOCRadar.

Family	Market Share / Volume	Distribution Method	Notable Development	Disruption Status
LummaC2	#1 by distribution volume (ANALYST INFERENCE, high confidence); 394,000+ Windows PCs infected in 60 days prior to May 2025 takedown (Microsoft); ~400% detection increase over prior 12 months	ClickFix fake CAPTCHA (PowerShell via Windows Run dialog); GitHub repos with AI-generated READMEs promoting cheats/exploits; malvertising; social media (YouTube, Facebook)	Post-May 2025 takedown: operators shifted from Cloudflare to Selectel (Russian-hosted) for C2; CastleLoader is primary delivery chain since Feb 2026 resurgence; fileless execution via .NET XOR decrypt-in-memory	Active — disrupted May 2025 by Microsoft/DOJ/Europol; infrastructure reconstituted within weeks
ACRStealer	Top-4 active distribution as of Feb 2026 (AhnLab ASEC); exact market share: No reliable data	Social engineering lures; cracked software distribution	No significant new development this cycle	Active — no disruption
StealC	Top-4 active; absorbed Lumma volume post-May 2025 disruption (Recorded Future); $200/month or $800/6-month MaaS subscription (SOCRadar)	Telegram MaaS subscription; social engineering	Growing market share as Lumma disruption beneficiary	Active — no disruption
Vidar	Top-4 active; $100-200/month subscription (Flare 2025); uses Telegram and Mastodon for C2 to blend into legitimate traffic	Social engineering; fake software; legitimate social media C2 abuse	Persistent macOS-targeting capability; cryptocurrency wallet theft emphasis	Active — no disruption
AMOS / Atomic Stealer	Significant macOS ecosystem expansion; no reliable market share percentage; includes persistent backdoor surviving reboots in latest versions	Fake macOS applications; cloned Homebrew installers; ClickFix-style DMG installers	Confirmed macOS expansion threat — no longer an 'emerging' concern	Active — no disruption
RedLine	Declining; legacy logs still circulating in underground markets	Phishing email attachments	Operational decline post-Operation Magnus (Oct 2024); logs remain live	Partially disrupted — logs still active

Family	Market Share / Volume	Distribution Method	Notable Development	Disruption Status
			credential threat for months post-infection	

5.2 Infostealer-to-IAB Pipeline Assessment

- Pipeline scale: 18.7 million infostealer logs collected between January and May 2026 in one sample study (Flare 2026). 54% of ransomware victims had domain credentials appear in stealer log marketplaces before the attack was detected at the victim organization — Source: Flare 2026.
- Timing data: Chainalysis 2026 identifies IAB on-chain inflow spikes typically preceding ransomware payment spikes by approximately 30 days. This 30-day lead-time window is the primary detection opportunity for enterprise defenders — organizations monitoring their credential exposure in stealer markets have a documented window to rotate credentials before ransomware deployment.
- Log pricing: Fresh logs (under 48 hours old) command 3-5x the commodity price due to live session token value. Average commodity log price $10/bot; corporate domain-admin credentials command significantly higher ($100-$3,000+).
- Infrastructure pivot risk: Lumma's migration from Cloudflare to Selectel (Russian-hosted) places the C2 layer in a jurisdiction with documented lower responsiveness to Western LE requests, materially reducing takedown probability for the next disruption attempt. This is the most actionable infrastructure signal in the stealer ecosystem this cycle.

SECTION 6 — FINANCIAL & INFRASTRUCTURE SIGNALS

6.1 Sanctions & Enforcement Actions

Date	Authority	Target	Rationale	Financial Exposure	Disruption Impact
May 20, 2026	OFAC / U.S. Treasury	Sinaloa Cartel fentanyl-to-crypto laundering network (Los Chapitos faction; Armando de Jesus Ojeda Aviles network); 11 individuals, 2 entities	Crypto-laundering of fentanyl proceeds; cash-to-crypto conversion moving U.S. drug sales to Mexico	Not publicly specified in SDN designation	Medium — financial cell disrupted; cartel has redundant laundering infrastructure
~May 18-27, 2026	Dutch FIOD (EU sanctions enforcement)	Stark Industries / WorkTitans BV / MIRhosting: 2 arrests — Youssef Zinad (57, Amsterdam) and Andrey Nesterenko (39, The Hague); 800+ servers seized	Providing economic resources to EU-sanctioned entities supporting Russian hybrid warfare; sanctions law violation (not cybercrime statutes — novel prosecutorial theory)	800+ servers seized; 5 locations raided (Enschede, Almere, Dronten, Schiphol-Rijk data centers)	High — primary Russian-aligned BPH platform dismantled; disrupts cyberattack staging, disinformation, and influence ops against EU states
April 24, 2026	OFAC / U.S. Treasury + Tether + LE	Central Bank of Iran (CBI) — 2 cryptocurrency addresses added to SDN List; Tether froze $344M in USDT linked to CBI-affiliated wallets	Sanctions evasion; state-directed financial flows	$344 million USDT frozen	High — largest single crypto freeze tied to state-nexus actor in window; demonstrates Tether's cooperative capacity with OFAC

6.2 Ransomware Financial Flow Observations

- FY 2025 aggregate: Total on-chain ransomware payments $820 million (down 8% YoY from $892 million in 2024). Median payment $59,556 — up 368% from $12,738 in 2024 — indicating a structural shift to fewer but larger payments. Source: Chainalysis 2026 Crypto Crime Report.
- Payment refusal: 69% of victims refused payment in 2025 (Verizon 2026 DBIR), up from 65% in 2024. Payment rates have collapsed from 76% (2019) to 28% (2026) — Kaspersky State of Ransomware 2026.
- Stablecoin dominance: 95% of illicit inflows to sanctioned entities/jurisdictions in 2025 transited stablecoins. Russia-linked sanctioned flows: $93 billion total in 2025; A7A5 token cluster alone: $72 billion. Source: TRM Labs 2026 Crypto Crime Report.
- IAB on-chain payments: At least $14 million tracked in 2025 — approximately 1.7% of total ransomware ecosystem on-chain flows. Source: Chainalysis.
- The Gentlemen specific cash-out (CONFIRMED, Check Point Research): ~800 transactions through 'buy desks' → Tinkoff bank QR code conversion to rubles (400,000 RUB / ~$4,400

minimum per transaction) → OTC physical cash delivery. Non-custodial wallets (Guarda, Trust Wallet, Exodus) used to avoid exchange-level KYC.

6.3 Infrastructure Hosting Patterns

- Stark Industries / WorkTitans BV: Operation assumed control of EU-sanctioned Stark Industries Solutions ASN after May 2025 sanctions failed to dislodge infrastructure by migrating to a Dutch-registered shell (WorkTitans BV / THE.Hosting brand). The FIOD sanctions-law prosecution (hosting provision as direct EU sanctions violation, not cybercrime) is a novel prosecutorial theory that if sustained creates precedent for EU liability against any ISP knowingly servicing sanctioned entities.
- Lumma C2 migration from Cloudflare to Selectel: Selectel is a commercially registered Russian hosting provider. This moves C2 infrastructure to a jurisdiction with documented lower Western LE cooperation responsiveness, increasing persistence vs. prior Cloudflare hosting. Actionable: see Section 11 leverage item F-2.
- First VPN exit node locations confirmed in LE action: U.S. nodes at 2.223.66.103, 5.181.234.59, 92.38.148.58; additional nodes across Australia, Belgium, France, Germany, Netherlands, Russia, Switzerland, Turkey, Ukraine, and 16 other countries.

SECTION 7 — LAW ENFORCEMENT & REGULATORY ACTIONS

7.1 May 2026 Actions

Operation	Lead Agency/Agencies	Date	Outcome	Ecosystem Impact
Operation Saffron	France, Netherlands (co-lead); Europol, Eurojust; 18 countries total; private sector: Bitdefender	May 19-20, 2026	33 servers seized across 27 countries; 1 operator arrested (Ukraine); domains 1vpns.com/.net/.org + Tor .onion variants seized; 83 intelligence packages on 506 identified users shared with partner countries; 5,000+ user accounts flagged in criminal traffic logs obtained	HIGH — removed primary anonymization layer used by 25 ransomware groups (incl. Avaddon, Phobos) for 12 years; 506 user exposures generate significant downstream case pipeline
Stark Industries / Dutch FIOD	Dutch FIOD (lead); European intelligence and financial crime partners	~May 18-27, 2026	~800 servers seized; 2 arrests — Youssef Zinad (57) and Andrey Nesterenko (39); 5 locations raided; ledgers, laptops, and mobile phones seized; charged under Dutch sanctions law	HIGH — dismantled primary EU-facing Russian-aligned cyberattack, disinformation, and influence operation staging platform; novel sanctions-law theory, if sustained, enables prosecution of European hosting enablers
Karakurt — Zolotarjovs Sentencing	U.S. DOJ (Southern District of Ohio)	May 6, 2026	Deniss Zolotarjovs (Latvian, 35) sentenced to 8.5 years; involved in $56M+ in losses across 54+ companies; DOJ confirmed gang used Russian government database access and paid military draft bribes to officials	MEDIUM — Karakurt largely inactive; establishes state-facilitation legal precedent for treating RU-nexus ransomware gangs as state-criminal enterprises
Operation Ramz (INTERPOL MENA)	INTERPOL; 13 MENA-region countries	Oct 2025 - Feb 2026 (announced May 17, 2026)	201 arrests; 382 suspects identified; 3,867 victims identified; 53 servers seized; phishing, malware, and cyber scam operations disrupted	MEDIUM — geographic expansion of LE cooperation; primarily fraud and social engineering rather than core

Operation	Lead Agency/Agencies	Date	Outcome	Ecosystem Impact
				ransomware infrastructure
BKA Identifies REvil/GandCrab Leaders	German Federal Criminal Police Office (BKA)	April 6, 2026	Public identification of Daniil Shchukin (UNKN, 31, Russian) and Anatoly Kravchuk (43, Russian-Ukrainian); 130 attacks in Germany; €35.4M ($40.8M) total damage; 25 cases, €1.9M paid; international arrest warrants issued (fugitives not in custody)	LOW-MEDIUM — legacy group inactive; intelligence and warrant value for network attribution

7.2 Reconstitution Status Tracker (180-Day Window)

Standing tracker updated monthly. Status as of May 31, 2026.

Operation	Action Date	Target	Action Type	30-Day Status	90-Day Status	180-Day Status
RAMP Forum Seizure	Jan 28, 2026	RAMP Russian-language ransomware forum	Forum seized; FBI splash page	Dark — no confirmed successor at 30 days	Dark — no primary confirmed successor at 90 days (anomalous)	Pending — 180-day status due July 28, 2026
BreachForums DB Exposure	Early 2026	BreachForums (323,986 member accounts)	DB resurfaced publicly; member data exposed	Partially active — platform operational under degraded trust	Partially active	Pending
LeakBase Seizure	March 2026	LeakBase data distribution platform	Seized	Not Reconstituted at 30 days	Pending — 90-day status due June 2026	Pending
BKA REvil Identification	April 6, 2026	REvil/GandCrab operators (2 individuals)	International arrest warrants issued; fugitives at large	No arrest at 30 days	Pending	Pending
Lumma Stealer LE Action	May 2025	Lumma C2 infrastructure (Microsoft/DOJ/Europol)	2,300 domains seized	Partially reconstituted — 3-6 months	Largely reconstituted — Selectel pivot confirmed	Fully Reconstituted — active at higher operational security

7.3 Cumulative Impact Assessment — May 2026

Short-term disruption (1-30 days): HIGH

Operation Saffron removed the anonymization layer for 25+ active groups simultaneously. Stark Industries dismantled the shared BPH platform used for Russian-nexus attack staging. The Gentlemen internal breach exposed operator identities creating an organic disruption event. The 9.4% MoM victim count decline in May is consistent with — though not exclusively attributable to — these events; seasonal variation and DLS publishing lag cannot be excluded.

Structural ecosystem impact (90+ days): MEDIUM

Historical reconstitution data is limiting: Lumma Stealer reconstituted within weeks post-May 2025 takedown; LockBit reconstituted as LockBit 5.0 within 8 months of Operation Cronos. Neither the Saffron nor the Stark seizure directly targeted RaaS platform operators — only enabling infrastructure. BPH customers will migrate within 1-7 days (historical pattern). The RAMP non-reconstitution at 120+ days is the one anomalous resilience-cost indicator; its cause (LE deterrence vs. private channel migration) will determine the structural significance of the January 2026 seizure.

SECTION 8 — VULNERABILITY EXPLOITATION MATRIX

Includes CVEs with confirmed or credible exploitation in ransomware/malware campaigns during the May 2026 reporting period. Sources: CISA KEV catalog (verified), THN (verified), Rapid7 blog, CERT-UA.

CVE	Product	CVSS	Exploitation Method & Post-Compromise	Threat Actor	Scale / Volume	CISA KEV	KEV Date / Notes
CVE-2026-20182	Cisco Catalyst SD-WAN Controller & Manager	10.0	Auth bypass; unauthenticated remote admin access; post-compromise: SSH key injection, NETCONF modification, root escalation, web shell deployment (XenShell, Godzilla, Behinder, Sliver C2, XMRig). 10 distinct clusters active since March 2026.	UAT-8616 (primary, Cisco-attributed); 9 additional clusters including cryptominers, credential stealers, Sliver C2	Global — 10 clusters, mass scale	YES	May 14-15, 2026; ~70-d exploitation before KEV listing
CVE-2025-61882	Oracle E-Business Suite v12.2.3-12.2.14	10.0	Unauthenticated RCE via HTTP; zero-day sold on RAMP forum by Cl0p-attributed actor; financial/HR data exfiltration for subsequent extortion	Cl0p (attributed, Rapid7)	Zero-day selling on RAMP; mass exploitation campaign likely imminent based on Cl0p historical pattern (MOVEit, GoAnywhere, Citrix Bleed)	Not confirmed in KEV as of May 31	CRITICAL C — Oracle E environmen unprotected KEV absent
CVE-2024-57726	SimpleHelp (remote support)	9.9	Missing authorization; low-priv technician creates admin API keys → privilege escalation to server admin; MSP-targeting vector	Multiple ransomware groups (MSP-targeting)	Actively exploited; federal deadline May 8, 2026	YES	Apr 25, 202 (~4-16 mon KEV lag fro 2024 discov
CVE-2024-57728	SimpleHelp	7.2	Path traversal (zip slip); admin uploads arbitrary files → RCE; co-exploited with CVE-2024-57726 in MSP environments	Multiple actors	Active; companion to CVE-2024-57726	YES	Apr 25, 202
CVE-2025-32433	Erlang SSH (Cisco context)	9.8	RCE via unauthenticated SSH; PoC shared in The Gentlemen's TOOLS channel; zeta88 and qbit actively evaluating for operational deployment	The Gentlemen (confirmed evaluation in leaked chats)	Evaluation phase — not yet at mass-exploitation scale	Confirm with CISA	Not confirm KEV as of reporting
CVE-2025-33073	NTLM relay (Active Directory)	N/A	NTLM relay attack; integrated into RelayKing standard reconnaissance workflow by The Gentlemen; systematic scanning	The Gentlemen	Systematic operational use in confirmed campaigns	Confirm with CISA	Not confirm KEV as of reporting

CVE	Product	CVSS	Exploitation Method & Post-Compromise	Threat Actor	Scale / Volume	CISA KEV	KEV Date / Notes
			documented in leaked operational chats				
CVE-2025-48700	Zimbra Collaboration Suite	6.1	Cross-site scripting → arbitrary JavaScript in user session; combined with CVE-2025-66376 for RCE chain; no user interaction required	UAC-0233 (Ukraine-targeting threat actor)	Active exploitation since Sept 2025 per CERT-UA; Ukraine-focused	YES	Apr 20, 202
CVE-2024-55591	Fortinet FortiOS management interface	9.8	Auth bypass on FortiOS management interface; explicitly referenced in The Gentlemen's internal CVE tracking alongside active FortiGate targeting operations	The Gentlemen (tracked for operational use)	Referenced alongside active FortiGate targeting	YES (prior period)	Prior to May 2026

KEV lag analysis: CVE-2026-20182 was actively exploited by 10+ clusters from March 2026 but KEV-listed May 14-15 — a ~70-day gap. CVE-2025-61882 (Oracle EBS, CVSS 10.0) is being sold as a zero-day exploit on RAMP with Cl0p attribution and is not yet in KEV — the most significant current KEV gap for organizations dependent on Oracle EBS in finance, HR, and supply chain. The SimpleHelp CVEs (assigned 2024) took 4-16 months to achieve KEV status despite active MSP-targeting exploitation. Organizations relying solely on KEV for patch prioritization are exposed in these pre-KEV windows.

SECTION 9 — SUPPLY CHAIN & THIRD-PARTY COMPROMISE

Campaign	Attacker	Compromised Component	Downstream Impact	Status
Mini Shai-Hulud / TanStack npm Worm	TeamPCP (linked to CipherForce ransomware group — TechCrunch/SafeDep)	TanStack/router GitHub repo; 42 @tanstack/* npm packages (84 malicious artifacts); worm propagated to 317 packages total across Antv (Alibaba), TanStack, and others in ~20 minutes	630 malicious versions across 317 packages; Mistral AI, UiPath, and 170+ downstream packages compromised; 2 OpenAI employee corporate devices compromised; credentials from GitHub Actions, AWS IMDS, HashiCorp Vault, Kubernetes exfiltrated	Detected by Socket AI Scanner within 6 minutes; malicious packages removed; CVE-2026-45321 assigned (Critical)
DAEMON Tools Installer Compromise	Unknown criminal actor	Official DAEMON Tools installers versions 12.5.0.2421-12.5.0.2434 (signed with legitimate developer certificates; distributed from official website)	~2.5 weeks of trojanized downloads (April 8 - late April 2026); downstream environment count: No reliable data	Remediated — clean installers released; affected version range documented
TrapDoor Campaign	Unknown (crypto/DeFi-targeting actor)	34+ malicious packages across 384+ versions on npm, PyPI, CratesIO; earliest activity May 22, 2026	Targets developers in crypto, DeFi, Solana, and AI; credential-stealing payload; downstream count: No reliable data	Ongoing as of May 31 — active removal effort
Glassworm Botnet (GitHub)	Glassworm threat actor	300+ GitHub repositories poisoned; malicious extensions on developer marketplaces; account hijacking via stolen credentials	Developer credential theft at scale; downstream count: No reliable data	Disrupted May 27, 2026 — CrowdStrike and Google coordinated takedown

Trend assessment: Verizon 2026 DBIR confirms nearly 30% of all data breaches now involve a third-party supplier — double the rate from 2024 (15%). Four confirmed supply chain incidents in a single reporting period is a notable clustering. The Mini Shai-Hulud campaign is technically the most significant: it demonstrates that OIDC-authenticated CI/CD pipelines can produce malicious packages with valid SLSA provenance, fundamentally undermining software supply chain integrity controls that organizations deployed as post-SolarWinds mitigations. The DAEMON Tools compromise is the most enterprise-relevant for traditional environments: a legitimately signed installer from the official vendor website bypasses all reputation-based defenses. TeamPCP's confirmed link to the CipherForce ransomware group means the CI/CD attack vector may soon feed ransomware deployments directly — ANALYST INFERENCE, medium confidence. CONFIRMATION SIGNAL: CipherForce DLS listing of a victim whose forensics identify initial access via CI/CD pipeline compromise.

SECTION 10 — ECOSYSTEM CONTROL NODE ANALYSIS

10.1 Top Control Nodes

A 'control node' is any entity whose disruption causes measurable cascading effects on other ecosystem participants.

Rank	Node	Type	Est. Ecosystem Reach	Dependencies	Single Point of Failure?	Disruption Difficulty
1	**Qilin RaaS**	RaaS Platform	~21% of Q1 2026 victims (445 YTD); 103/month; 26 confirmed healthcare victims (17% of all healthcare DLS listings); formal BreachForums partnership — CONFIRMED	Exploit.in/XSS.is forums; BPH infrastructure; affiliate network; cryptocurrency cashout	Partial — distributed affiliate model; no single physical node; operator identity not public	High — Russian/CIS nexus suspected; no jurisdiction with enforcement authority has acted
2	**The Gentlemen RaaS**	RaaS Platform	~15% of 2026 YTD victims (~332); #2 operator; admin identity now partially exposed — THRESHOLD MET	4VPS (compromised); zeta88/hastalamuerte identity now partially known; Selectel-adjacent infrastructure	Partial — 9 operators identified; admin identity and TOX ID now public	Medium-Low — immediate enforcement window open; see Section 11 leverage item I-1
3	**DarkForums**	Forum / IAB Market	ANALYST INFERENCE, medium confidence: 30-40% of premium IAB listings now flow through DarkForums (Rapid7 H2 2025: 221 threads, highest average base prices); grew 600% during BreachForums collapse	Server infrastructure; admin identity; cryptocurrency payment rails; user reputation system	Partial — admin arrest could displace listings; marketplaces reconstitute in 4-8 weeks	High — English-language; potentially reachable by Western LE if hosted in cooperative jurisdiction
4	**Stablecoin Cashout Infrastructure (USDT/A7A5)**	Crypto Laundry	$93B in sanctioned-entity flows (2025, TRM Labs); A7A5 token: $72B; 95% of illicit inflows to sanctioned entities transit stablecoins;	Tether Limited (USDT issuer); correspondent banking relationships; stablecoin issuance infrastructure	Partial — Tether is the realistic chokepoint; alternatives exist but immature at required scale for Russian ops	Extreme — requires regulatory action vs. Tether or stablecoin issuers; see Section 11 leverage item F-3

Rank	Node	Type	Est. Ecosystem Reach	Dependencies	Single Point of Failure?	Disruption Difficulty
			entire ransomware payment collection chain depends on USDT access			
5	**LummaC2 MaaS**	Stealer Service	ANALYST INFERENCE, high confidence: #1 infostealer by distribution volume; 394,000+ Windows PCs infected in 60 days pre-May 2025 takedown (Microsoft); drives majority of credential-to-IAB pipeline	Selectel hosting (post-Cloudflare pivot); Telegram/forum marketing; CastleLoader delivery network	Partial — demonstrated resilience to takedown; reconstituted within weeks of May 2025 Microsoft/DOJ action	High — Russian origin; Selectel pivot to RU jurisdiction; see Section 11 leverage item F-2
6	**IAB Pipeline (Stealer Log Markets)**	IAB Market	ANALYST INFERENCE, medium confidence: 54% of ransomware victims had credentials in stealer markets before attack; $14M+ on-chain IAB payments (Chainalysis 2025); 18.7M logs Jan-May 2026 (Flare)	Distributed Telegram channels; dark web marketplaces; infostealer malware families	No — hundreds of channels; no single admin	Extreme — decentralized; no single LE enforcement mechanism; disruption requires sustained coordinated pressure
7	**LockBit 5.0**	RaaS Platform	~8% Q1 2026 (163 victims); demonstrated high reconstitution capacity (Feb 2024 disruption → LockBit 5.0 in 8 months)	Affiliate network; cross-platform tooling; operator 'LockBitSupp' (Dmitry Khoroshev, identified 2024)	Partial — prior disruption reconstituted; brand demonstrated extreme resilience	High — distributed affiliates; primary operator in Russia, beyond arrest reach

10.2 Cascade Failure Analysis

Node: The Gentlemen RaaS (Rank 2) — HIGHEST IMMEDIATE LEVERAGE

- What breaks downstream: 9 identified operators lose coordination; 8 affiliate TOX IDs lose platform access; ~332 YTD victim pipeline disrupts; dual-leverage extortion tactic documented by CPR is disrupted. Secondary: affiliate talent migrates to Qilin or DragonForce, accelerating those groups.

- Realistic reconstitution timeline: 60-120 days based on historical RaaS averages, but faster if admin retains builder source code. Admin's AI-assisted development capability (panel built in 3 days) means rebuild is faster than traditional groups.
- Enforcement mechanism: Admin zeta88/hastalamuerte partially deanonymized via leaked TOX ID and shadow file. International warrant issuance against identified operators is feasible within weeks. THRESHOLD MET — act within 30-60 day window.

Node: Stablecoin Cashout Infrastructure (Rank 4) — HIGHEST STRUCTURAL LEVERAGE

- What breaks downstream: Guaranteed USDT access is the structural dependency for the entire ransomware payment ecosystem. Restricting USDT to sanctioned wallet addresses or mandating on-chain compliance checks by Tether would impair payment collection across all active RaaS groups simultaneously. Forces groups back to Bitcoin (more traceable) or extends victim negotiation windows due to cashout friction.
- Realistic reconstitution timeline: 90+ days for structural impact; no realistic reconstitution path if stablecoin issuers enforce wallet-level screening.
- Enforcement mechanism: OFAC designation of A7A5 token under CAATSA; Treasury regulatory guidance requiring Tether to implement SDN list wallet screening under penalty of USD correspondent banking access loss.

Node: Qilin RaaS (Rank 1) — HIGHEST VOLUME LEVERAGE

- What breaks downstream: 21% of global ransomware volume disrupted; 26 healthcare victims per year lose primary adversary; BreachForums partnership reaching 300,000+ users loses RaaS technical infrastructure. Displaced affiliates migrate to DragonForce/The Gentlemen within 30-60 days.
- Realistic reconstitution timeline: 30-60 day victim count impact; full affiliate migration within 60-90 days. LockBit model suggests multi-quarter disruption if operator identity is confirmed and arrests follow.
- Enforcement mechanism: No confirmed operator identity in public domain. Requires HUMINT penetration of affiliate network or infrastructure-level disruption via ISP coordination.

10.3 Structural Vulnerability Summary

The single most critical structural weakness in the current ecosystem is the dependence of the entire payment collection chain on stablecoin infrastructure — primarily USDT via the A7A5 token cluster. With 95% of illicit ransomware-related flows using stablecoins ($72B A7A5 alone per TRM Labs 2026), Tether Limited represents an unprecedented concentration of financial chokepoint leverage for law enforcement. The ecosystem is most brittle here because: (1) ransomware groups cannot collect payment without it; (2) Tether operates in a Western-accessible jurisdiction; and (3) existing BSA/AML regulatory frameworks already apply — they are simply not enforced at the wallet-screening level required. Simultaneously, The Gentlemen admin identity disclosure creates a rare narrow-window opportunity to decapitate a top-3 operator with confirmed identity intelligence. These two leverage mechanisms are independent and should be pursued in parallel: one is an immediate 30-day tactical action; the other is a 12-18 month regulatory campaign.

SECTION 11 — STRATEGIC LEVERAGE ASSESSMENT

Rule 3 format throughout. No 'monitor,' 'assess,' or 'watch' language. All items use trigger/condition/threshold/action/window structure.

11.1 Financial Pressure Points

LEVERAGE F-1: The Gentlemen Cryptocurrency Cash-Out Infrastructure

- **TARGET:** Tinkoff bank QR code cash-out pathway; OTC physical cash delivery network; exchange chain ('buy desk') infrastructure identified in The Gentlemen's leaked chats.
- **CONDITION:** Admin zeta88 confirmed using Tinkoff QR cash-out (400,000 RUB minimum / ~$4,400 per transaction) and OTC delivery. ~800 transactions through buy desks documented. Confirmed in verified source (Check Point Research, May 13, 2026).
- **THRESHOLD:** THRESHOLD MET — cash-out methodology documented and publicly reported. Admin knows the data is compromised and may be migrating infrastructure.
- **ACTION:** File STR with FinCEN citing Check Point TOX IDs and wallet addresses; initiate OFAC designation review for identified non-custodial wallets (Guarda, Trust Wallet, Exodus infrastructure used by zeta88); provide TOX ID F8E24C7F... to Five Eyes partners for SIGINT/HUMINT correlation; alert Tinkoff compliance team via FinCEN SAR referral mechanism.
- **WINDOW:** 30-60 days maximum before admin migrates all financial infrastructure following acknowledgment of the breach.
- **PRIORITY:** Critical

LEVERAGE F-2: Selectel OFAC Designation (Lumma C2 Host)

- **TARGET:** Selectel (Russian hosting provider) — confirmed new Lumma Stealer C2 infrastructure post-Cloudflare pivot.
- **CONDITION:** Lumma confirmed migrated C2 to Selectel post-May 2025 disruption. Selectel is commercially registered with international payment infrastructure.
- **THRESHOLD:** THRESHOLD MET — migration confirmed in verified reporting. Each day of inaction allows stealer-to-IAB pipeline to continue at scale.
- **ACTION:** Initiate OFAC designation review for Selectel as a facilitating entity under cyber-related executive orders; engage Selectel's upstream tier-1 ISP connectivity providers (Western-accessible) to enforce abuse policies; coordinate with Europol for parallel action.
- **WINDOW:** Ongoing; most effective before Lumma migrates to a second alternative provider.
- **PRIORITY:** High

LEVERAGE F-3: USDT/Tether Stablecoin Wallet Screening Mandate

- **TARGET:** Tether Limited (USDT issuer) and A7A5 token infrastructure — the structural ransomware payment chokepoint.

- **CONDITION:** 95% of illicit flows to sanctioned entities in 2025 transited stablecoins; A7A5 token alone: $72 billion in illicit stablecoin flows (TRM Labs 2026); USDT is the confirmed cashout mechanism for major Russian-aligned operators.
- **THRESHOLD:** THRESHOLD MET — $72B A7A5 flow and $93B total sanctioned-entity stablecoin exposure already exceeds any reasonable action threshold.
- **ACTION:** OFAC shall designate the A7A5 token as blocked property under 31 CFR Part 510 (CAATSA Russia sanctions); Treasury shall issue regulatory guidance requiring Tether to implement wallet-level SDN list screening before USDT issuance/redemption under penalty of USD correspondent banking access loss; FinCEN shall issue Geographic Targeting Order covering Tether transactions above $3,000 involving Russia-linked exchanges.
- **WINDOW:** 12-18 months before alternative payment rails (CBDCs, privacy coins) become operationally viable for Russian ransomware operators at scale; acting now imposes maximum friction while alternatives are immature.
- **PRIORITY:** Critical — highest-impact available financial leverage in the ecosystem

11.2 Infrastructure Pressure Points

LEVERAGE I-1: The Gentlemen Admin Identity (zeta88 / hastalamuerte)

- **TARGET:** RaaS administrator partially deanonymized via May 4 backend breach; TOX ID: F8E24C7F5B12CD69C44C73F438F65E9BF560ADF35EBBDF92CF9A9B84079F8F04060FF98D098E; shadow file entry 'zeta88' confirmed; 4VPS hosting link.
- **CONDITION:** Admin identity exposed. Admin acknowledged breach publicly and is actively rebuilding operational security. Every week without action allows migration and identity hardening.
- **THRESHOLD:** THRESHOLD MET — identity exposure already occurred May 4. Enforcement window is narrowing.
- **ACTION:** Transmit TOX ID and shadow file hashes to Five Eyes partners for HUMINT and SIGINT correlation; issue international arrest warrant via Interpol Red Notice; coordinate with Eastern European partner services for physical location determination based on communication metadata; request 4VPS hosting provider records via MLAT.
- **WINDOW:** 30-60 days maximum before full operational security rebuild. Admin announced infrastructure overhaul on May 4 itself.
- **PRIORITY:** Critical

LEVERAGE I-2: Post-Stark Industries BPH Migration Window

- **TARGET:** Stark Industries / WorkTitans BV customers migrating to alternative BPH providers within days of May seizure.
- **CONDITION:** FIOD seized 800 servers; First VPN 506-user list in LE possession. Historical pattern: BPH customers migrate within 1-7 days. Customer lists from Stark Industries servers may identify overlapping actors.
- **THRESHOLD:** Migration window is OPEN NOW — most acute in first 14 days post-seizure (~by June 10, 2026).

- **ACTION:** Cross-reference Stark Industries server logs (FIOD custody) against First VPN 506-user list and known ransomware group infrastructure IOCs; identify migration destinations via BGP monitoring of Russian-adjacent ASNs receiving new traffic from previously Stark-hosted IPs; transmit identified new hosting providers to Europol for secondary action.
- **WINDOW:** 14 days — by approximately June 10, 2026.
- **PRIORITY:** High

LEVERAGE I-3: Operation Saffron Intelligence Package Follow-On (90-Day Window)

- **TARGET:** Active ransomware operators among the 506 identified First VPN users; 83 intelligence packages in partner country hands.
- **CONDITION:** Intelligence packages shared with 27 countries. First VPN operator logs document criminal traffic from 506 users. Historical VPN service reconstitution: 60-90 days.
- **THRESHOLD:** Threshold for action: identification of 3+ operators correlating to active ransomware victim DLS listings within the 83 intelligence packages.
- **ACTION:** Europol EC3 shall coordinate cross-referencing of 83 intelligence packages against active ransomware case files within 90 days of Saffron takedown; any operators identified in arrestable jurisdictions shall be subject to immediate MLAT requests; identified infrastructure providers shall be referred to ISPs for network suspension.
- **WINDOW:** 90 days from Operation Saffron (by ~August 18, 2026) before suspects migrate to successor VPN infrastructure and re-anonymize.
- **PRIORITY:** Critical

11.3 Jurisdictional Pressure Points

LEVERAGE J-1: Russian Deliberate Non-Enforcement — State-Facilitation Argument with SORM Evidentiary Basis

- **TARGET:** Russian federal government as the enabling actor for RU-nexus ransomware operators (Qilin, LockBit, The Gentlemen, Akira); diplomatic, financial, and legal pressure mechanisms.
- **CONDITION:** Three confirmed evidentiary pillars now support the deliberate non-enforcement argument as a policy position rather than a capability gap: (1) SORM architecture — Russian law requires all ISPs to install FSB-controlled intercept hardware, giving the FSB real-time visibility into all Russian-IP traffic; the FSB can observe ransomware operator communications, infrastructure, and financial flows in real time. (2) Karakurt/Zolotarjovs DOJ documentation (May 6, 2026) — gang used Russian government database access and paid military draft bribes; confirms active state-criminal relationship, not passive tolerance. (3) SORM + deliberate non-enforcement: Russian authorities have categorical technical capability to identify and disrupt domestic ransomware operators and have chosen not to. This is a policy posture, not a surveillance gap.
- **THRESHOLD:** THRESHOLD MET — all three evidentiary pillars are established. The April 2026 VPN crackdown and associated banking system disruption (reported; see Section 12) provides the sharpest available illustration: Russia accepted macroeconomic self-harm from VPN-dependent banking failures to enforce internet control objectives, while simultaneously operating a permissive

environment for ransomware infrastructure. This is not an oversight — it is a documented policy trade-off.

- **ACTION:** DOJ/NSD shall formally designate deliberate non-enforcement of SORM-visible ransomware operators as a state-facilitation finding in indictments against Qilin and LockBit operators; State Department shall incorporate SORM non-enforcement evidence into bilateral diplomatic communications with Russian counterparts; Five Eyes intelligence community shall produce a coordinated public assessment attributing RU-nexus ransomware permissiveness to confirmed FSB technical capability combined with deliberate non-action — shifting the diplomatic framing from 'Russia can't' to 'Russia won't.'
- **WINDOW:** Ongoing; SORM evidence base is standing. April 2026 VPN crackdown banking failure is a fresh illustration that strengthens the policy-choice argument while events remain in public memory.
- **PRIORITY:** High

11.4 Coming Month Focus — Top 3 Priority Actions (June 2026)

1. [CRITICAL] Act on The Gentlemen admin identity disclosure — 30-day window.

Expected outcome: Arrest or flight-forcing of zeta88/hastalamuerte; disruption of the ~332-victim YTD pipeline; intelligence windfall from full 16.22 GB Rocket DB; potential dismantlement of 8 confirmed affiliate operations.

2. [CRITICAL] OFAC: initiate A7A5 token and Tether wallet-screening regulatory action.

Expected outcome: $72B+ annual illicit flow disruption if sustained; forces Russian ransomware operators into less liquid cryptocurrency alternatives, extending cashout timelines from days to weeks and creating new traceability opportunities.

3. [HIGH] Cross-reference Stark Industries server logs against First VPN 506-user list before June 10.

Expected outcome: Identification of Russian-nexus actors using both services simultaneously; 10-50+ actionable investigative leads; potential identification of previously unknown ransomware group infrastructure.

SECTION 12 — UNCONFIRMED SIGNALS & HORIZON INDICATORS

- **[UNCONFIRMED REPORTING] Cl0p Mass Exploitation Campaign via CVE-2025-61882 (Oracle EBS, CVSS 10.0):** CVE-2025-61882 is being sold on RAMP forum by a Cl0p-attributed actor (Rapid7 blog). Cl0p's historical mass-exploitation pattern (MOVEit, GoAnywhere, Citrix Bleed) involves zero-day purchase followed by simultaneous mass-exploitation of thousands of vulnerable systems. CONFIRMATION SIGNAL: Mass Oracle EBS victim notifications or Cl0p DLS listings; Oracle emergency security advisory. REFUTATION SIGNAL: Oracle patch released and CVE added to KEV before observed Cl0p DLS listings.
- **[ANALYST INFERENCE — HIGH CONFIDENCE] First VPN Successor Service Launch:** Based on historical reconstitution patterns (Lumma: weeks; Hydra: 12 months; similar VPN services: 60-90 days), a First VPN successor anonymization service is likely to emerge by August 2026. CONFIRMATION SIGNAL: Dark web advertising of a new VPN service with similar pricing and capability profile; forum discussions on XSS/RAMP about replacement services. REFUTATION SIGNAL: No successor advertising by September 1, 2026, suggesting permanent migration to private channels.
- **[ANALYST INFERENCE — MEDIUM CONFIDENCE] RAMP Non-Reconstitution Significance:** The 120+ day absence of a primary Russian-language RaaS coordination forum is anomalous. Competing explanations: (1) LE infiltration deterring reconstitution attempts; (2) permanent migration to private invite-only channels invisible to open-source collection. The latter is more operationally concerning as it reduces LE and researcher visibility into ecosystem coordination. CONFIRMATION SIGNAL: New Russian-language ransomware forum with verifiable RaaS operator posts on XSS or Exploit by June 2026. REFUTATION SIGNAL: Continued absence through July 2026, supporting private migration hypothesis.
- **[UNCONFIRMED REPORTING] Qilin Healthcare Targeting Escalation:** Qilin's 26 confirmed healthcare victims in 2026 YTD represents 17% of all healthcare DLS listings (LinkedIn healthcare advisory, May 2026). If pace continues through Q2, Qilin becomes the #1 ransomware threat to healthcare globally. CONFIRMATION SIGNAL: Healthcare victim count exceeding 35 in a single month; DLS listing of a Tier 1 hospital network (500+ beds). REFUTATION SIGNAL: Significant LE action against Qilin infrastructure or shift in affiliate targeting instructions.
- **[ANALYST INFERENCE — MEDIUM CONFIDENCE] TeamPCP/CipherForce CI/CD-to-Ransomware Pipeline:** TeamPCP (Mini Shai-Hulud attacker) is also linked to CipherForce ransomware group (TechCrunch/SafeDep, May 2026). No confirmed ransomware deployment using CI/CD attack vector confirmed as of report date. CONFIRMATION SIGNAL: CipherForce DLS listing of a victim whose forensics identify initial access via CI/CD pipeline compromise. REFUTATION SIGNAL: CipherForce DLS remains empty through June 30, 2026.
- **[UNCONFIRMED REPORTING] Russia April 2026 VPN Crackdown — Banking System Disruption:** Reporting indicates that Russia's April 2026 enforcement action against VPN services — executed via TSPU (Technical Means for Countering Threats) deep packet inspection infrastructure deployed by Roskomnadzor — caused collateral disruption to banking system connectivity, with VPN-dependent payment processing and interbank communications experiencing outages. If confirmed, this event is analytically significant not for its cybercrime ecosystem impact but for what it demonstrates about Russian state behavior: Russia accepted verifiable macroeconomic self-harm from infrastructure control enforcement while simultaneously operating a permissive environment for ransomware operators whose FSB visibility under SORM is equally

complete. This is the sharpest available evidence that ransomware non-enforcement is a deliberate policy trade-off, not a governance failure. CONFIRMATION SIGNAL: Russian financial sector reporting of payment processing outages correlated with Roskomnadzor VPN enforcement dates; TSPU blocking logs referencing VPN service IPs active in April 2026. REFUTATION SIGNAL: No corroborated reporting of banking connectivity disruption linked to the VPN enforcement action from multiple independent Russian financial media sources.

- **[CREDIBLE REPORTING] FIFA World Cup 2026 Credential Harvesting Risk:** CTM360 documented 11,000+ fake government portals in a GovTrap campaign targeting FIFA 2026 attendees (May 2026); specific targeting attribution (sectors, sponsors, harvesting methods) was not available in verified sources this cycle and is insufficient for a full indicator entry. Note only: World Cup-affiliated organizations should treat June-July 2026 as an elevated phishing risk window.

SECTION 13 — ANALYTIC CAVEATS & COLLECTION GAPS

13.1 Sources Blocked or Inaccessible During Collection

The following sources were unavailable or returned no substantive content via web_fetch and are excluded from the citation pool (Standing Rule 5). Information attributed to these sources in this report was corroborated via other verified sources or credited as search-result-only attribution:

- bleepingcomputer.com — Specific Stark Industries URL returned empty response (JavaScript-rendered). Stark Industries coverage sourced from corroborating search snippets and Perplexity intelligence integration.
- halcyon.ai — The Gentlemen threat assessment URL returned empty response. Halcyon data corroborated via Check Point Research verified source.
- securityweek.com — Stark Industries arrest URL returned empty response.
- ransomware.live homepage — JavaScript-rendered; /stats/2026 subpage fetched separately and verified.
- ofac.treasury.gov/recent-actions — No cybercrime-specific designations found beyond Sinaloa Cartel action; Iran CBI designation sourced from Chainalysis blog search snippet.
- ic3.gov — No monthly report available; IC3 publishes annual Internet Crime Reports only.
- mandiant.com, secureworks.com, crowdstrike.com blogs — Not individually fetched; no specific May 2026 reports identified via search.

13.2 Data Unavailable or Unreliable This Cycle

- May 2026 final victim count: Month-close figure not yet confirmed. The ~700 estimate and 9.4% MoM decline are directionally reliable from Ransomware.live tracking but will update at month close.
- Per-group May-specific victim counts: April actuals (Breachsense) are the most current confirmed monthly figures. May counts are estimated from DLS tracking.
- Average ransom payment for May 2026: No monthly figure. Most current is Chainalysis FY 2025 ($820M total, $59,556 median).
- Time-to-publish (leak site signal): Per-incident compromise-to-publication lag not systematically tracked in open sources this cycle — a persistent collection gap.

13.3 Known Biases in Victim Count Data

- Inflation bias: Groups list victims even when no ransom is paid; some victims are re-listed after non-payment. Check Point Q1 2026 estimates 3-5% of DLS listings are re-listings.
- Deflation bias: Victims who pay and whose data is not published are systematically undercounted — estimated 15-30% of actual attack volume goes unreported on DLS (ANALYST INFERENCE, low confidence). True victimization rate is higher than DLS counts.

- Reporting lag bias: Recently compromised victims may take 30-90 days to appear on DLS. May 2026 counts will grow retroactively.
- Geolocation bias: U.S. over-representation in IAB listings (30.9% per Rapid7) is reinforced by English-language researcher focus. Non-English-speaking markets (Brazil, India, Southeast Asia) are systematically under-reported in Western threat intelligence sources.

13.4 Competing Explanations for Major Observed Trends

- May 2026 victim count decline (9.4% MoM): Could reflect Operation Saffron/Stark disruption OR seasonal variation OR DLS publishing lag. Without a multi-year May baseline, LE attribution is ANALYST INFERENCE, medium confidence.
- IAB base price jump (+4,055% Rapid7 H2 2025): May partially reflect Rapid7's expanded sampling to DarkForums and RAMP (first inclusion) rather than genuine price inflation. DarkForums premium listings significantly skew the average upward.
- Encryption-free extortion growth: Could reflect genuine strategic shift OR improved detection/reporting of exfiltration-only incidents previously undercounted OR pre-encryption extortion pressure being misclassified as encryption-free. Current data does not differentiate these models reliably.

SOURCES

Verified sources (fetched and confirmed): starred (*). All others contributed via search-result-level attribution per Section 13.1.

Ransomware Tracking Platforms

- * ransomware.live/stats/2026 — YTD 2026 statistics, new groups table [verified May 31, 2026]
- Breachsense April 2026 Ransomware Report — April victim counts, sector/geography breakdowns [search-result attribution]

Vendor Threat Intelligence

- * Check Point Research — The State of Ransomware Q1 2026 (May 11, 2026): research.checkpoint.com/2026/the-state-of-ransomware-q1-2026/
- * Check Point Research — Thus Spoke...The Gentlemen (May 13, 2026): research.checkpoint.com/2026/thus-spoke-the-gentlemen/
- Rapid7 — H2 2025 Initial Access Broker Report (March 2026) [search-result attribution]
- S-RM — 2026 Cyber Incident Insights Report [search-result attribution]
- Flare — 2026 State of Enterprise Infostealer Identity Exposure (May 25, 2026) [search-result attribution]
- TrendMicro — LummaC2 resurgence analysis [search-result attribution]
- Kaspersky — State of Ransomware 2026 (May 11, 2026) [search-result attribution]

Government & Law Enforcement

- * The Hacker News — First VPN Dismantled (Operation Saffron), May 22, 2026: thehackernews.com/2026/05/first-vpn-dismantled-in-global-takedown.html
- * The Hacker News — CISA Adds CVE-2026-20182 to KEV, May 15, 2026: thehackernews.com/2026/05/cisa-adds-cisco-sd-wan-cve-2026-20182.html
- * The Hacker News — BKA Identifies REvil Leaders, April 6, 2026: thehackernews.com/2026/04/bka-identifies-revil-leaders-behind-130.html
- CISA KEV Catalog — April-May 2026 additions [search-result attribution]
- CERT-UA — CVE-2025-48700 Zimbra advisory [search-result attribution]

Cybersecurity News

- * TechCrunch — DOJ says ransomware gang tapped into Russian government databases (May 6, 2026): techcrunch.com/2026/05/06/doj-says-ransomware-gang-tapped-into-russian-government-databases/

- Verizon 2026 DBIR — Ransomware payment statistics [search-result attribution]
- TechCrunch / SafeDep / StepSecurity — Mini Shai-Hulud TanStack npm worm (May 19-20, 2026) [search-result attribution]
- techtimes.com, hackread.com — Stark Industries Netherlands FIOD seizure [search-result attribution; BleepingComputer URL failed fetch]

Financial Intelligence

- Chainalysis 2026 Crypto Crime Report (February 2026; FY 2025 data) — $820M total, $59,556 median, $14M IAB on-chain [search-result attribution]
- TRM Labs 2026 Crypto Crime Report — $93B sanctioned-entity flows, A7A5 $72B, 95% stablecoin [search-result attribution]