Unknown Title

Executive Summary

The Russian cybercriminal ecosystem is undergoing a period of profound transformation, shaped by unprecedented international law enforcement campaigns, shifting domestic enforcement priorities, and enduring ties between organized crime and the Russian state. Operation Endgame, launched in May 2024, targeted ransomware operators, money laundering services, and affiliate infrastructure across multiple Russian jurisdictions. In response, Russian law enforcement agencies have carried out a series of high-profile arrests and seizures. These events mark a departure from Russia's traditional posture of near-total noninterference in domestic cybercrime, complicating the long-held perception of Russia as a blanket "safe haven" for cybercriminals. Leaked chats and investigative reporting reveal that senior figures within these threat groups often maintained relationships with Russian Intelligence Services, providing data, performing tasking, or leveraging bribery and political connections for impunity.

Within the underground, this has eroded trust, as affiliates complain of scams, impersonation, and selective law enforcement pressure. These shifts have, in turn, accelerated operational changes, from stricter vetting in ransomware-as-a-service (RaaS) programs to ransomware groups rebranding and adopting decentralized communication platforms to mitigate perceived infiltration risks. At the same time, Western governments are hardening their policies against ransomware, moving toward bans on ransom payments, mandatory reporting of incidents, and even offensive cyber operations designed to neutralize adversary infrastructure before attacks occur. This more aggressive stance has coincided with prisoner swaps and negotiations that highlight how high-value cybercriminals function as political assets within Russia's broader geopolitical calculus.

Dark Covenant 3.0 situates these developments within the broader context of state-criminal interaction in Russia. Cybercrime in this environment cannot be understood solely as a commercial enterprise; it is also a tool of influence, a means of information acquisition, and a liability when it threatens domestic stability or undermines Russian interests. The trajectory of this ecosystem will depend on how Russian authorities balance external pressure, domestic political sensitivities, and the enduring strategic value derived from cybercriminal proxies.

Key Findings

- Recorded Future intelligence shows that the Russian government's relationship with cybercriminals has evolved from passive tolerance to active management. Since 2023, Insikt Group has identified a measurable shift in how Russian authorities engage with cybercriminal groups: selective enforcement, choreographed arrests, and public "examples" used to reinforce state authority.
- Leaked communications analyzed by Insikt Group expose direct, tasking-level coordination between cybercriminal leaders and Russian intelligence intermediaries.
- Recorded Future dark web collections indicate the Russian cybercriminal underground is fracturing under the dual pressures of state control and internal mistrust, while proprietary forum monitoring and ransomware affiliate chatter show increasing paranoia among operators.
- Recorded Future data reveals how Russian cybercriminal groups are decentralizing operations to evade both Western and domestic surveillance.
- Insikt Group assesses that Russia is now strategically leveraging cybercriminals as geopolitical instruments, as recent observations tie Russian cybercriminal detentions and releases to broader diplomatic cycles.

Methodology

This report narrowly examines the "Dark Covenant" framework — defined and discussed in Insikt Group reports from 2021 and 2023 — between 2024 and 2025. This includes the spectrum of direct, indirect, and tacit relationships between Russia-based (or Russia-aligned) cybercriminal threat actors and elements of the Russian state, and how those relationships adapted under sustained Western pressure from Operation Endgame and related counter-ransomware actions. Our focus is primarily on entities targeted by Operation Endgame, and our temporal scope centers on May 2024 (when Operation Endgame started) through September 2025, with limited historical baselining to prior episodes evidencing state-criminal proximity. This includes Operation Endgame's actions and subsequent Russian enforcement timelines that illuminate which services or threat actors were targeted by rather than shielded from law enforcement.

The report synthesizes: (1) public law-enforcement releases and Operation Endgame materials that enumerate targeted malware families, botnets, and money-movement services; (2) Russian legal, prosecutorial, and media statements that document arrests, seizures, and sentencing; and (3) dark web forum and Telegram communications that reveal underground reactions, trust dynamics, and operational adaptations. We also reference leaked chat archives and investigative reporting relevant to Conti and Trickbot and associated facilitators, where they illuminate alleged protection, information sharing, or tasking

with state entities. This report also incorporates transnational policy developments and diplomatic events (for example, prisoner exchanges involving high-value Russian cybercriminals) to contextualize how external pressure intersects with Russia's domestic calculus of protection and control. All such events are treated as indicators, not dispositive proof, of Russian state priorities and leverage.

Background

Dark Covenant

The "Dark Covenant" framework describes the web of relationships linking Russia's cybercriminal underground to elements of the state, especially intelligence and law enforcement services, through a spectrum of direct ties, indirect affiliations, and tacit understandings. The original Dark Covenant report, published on September 9, 2021, argued that these relationships are longstanding and fluid; recruitment of skilled criminals (sometimes under threat of prosecution), selective protection, and the state's ability to see and shape parts of the underground create an ecosystem in which cybercrime can persist when it serves state interests. Crucially, the report formalized three categories of linkage — direct associations, indirect affiliations, and tacit agreement — and emphasized that the absence of meaningful punitive action often signals tolerance or approval from the Kremlin.

Dark Covenant 2.0, released January 31, 2023, extended the model into wartime. It found that Russia's full-scale invasion of Ukraine catalyzed visible shifts in the underground. Some threat groups openly pledged allegiance to the Kremlin, others splintered or rebranded, and "hacktivist" auxiliaries amplified information operations alongside cyberattacks. Insikt Group assessed that cybercriminal tools, infrastructure, and tactics, techniques, and procedures (TTPs) supplied plausible deniability for state operations, while headline arrests and forum bans looked more like reputation management than a genuine break with cybercrime. The 2023 report reaffirmed the three-tier linkage model and documented how war pressures deepened certain connections while obscuring others.

Across both reports, the throughline is not a single command-and-control structure but a pragmatic bargain. Russian services recruit or co-opt talent when useful, look the other way when activity aligns with state aims, and selectively enforce laws when threat actors become politically inconvenient or externally embarrassing. This "covenant" blends incentive, intimidation, and opportunism, producing a resilient gray zone where criminal enterprise doubles as an instrument of statecraft.

Dark Covenant 3.0 situates that bargain in the post-Operation Endgame era. The same ecosystem now operates under heavier international pressure, new domestic optics, and a more explicit politics of protection. The core construct remains intact — direct, indirect, and tacit bonds — but the edges have sharpened, with selective Russian crackdowns on low-utility enablers and continued insulation for threat groups that offer intelligence or geopolitical value. This report uses that lens to explain why Russia appears less like a uniform "haven" and more like a managed market — one where state interests, not law, determine who gets protected and who does not.

Operation Endgame

Operation Endgame was more than a multinational takedown — it was a public test of how far Western pressure can reach into an ecosystem where Russian cybercrime and elements of the state have long coexisted under a pragmatic "politics of protection." In May 2024, Europol publicly announced the start of Operation Endgame, an initiative targeting ransomware precursors, specifically loader malware. However, based on the success of their first day of action in May 2024, Europol expanded its mandate to include other elements of the ransomware supply chain.

Operation Endgame was divided into two "seasons": one set of major takedowns in May 2024, and the other in May 2025. In practice, those seasons bundled coordinated actions against loaders and enablers (for example, IcedID, SystemBC, Pikabot, SmokeLoader, Bumblebee, and others), classic botnets and bankers (Trickbot, Qakbot, DanaBot, Emotet, and others), and money-movement infrastructure (Cryptex, Universal Automated Payment Service [UAPS], PM2BTC, and others), alongside public designations like the European Union (EU) "Most Wanted" entries tied to Conti and Trickbot figures. A key element of the seasons was the release of targeted videos intended to intimidate threat actors to come forward with information. The decision to pair technical disruption with naming-and-shaming videos signaled an influence campaign aimed at affiliates and suppliers, accelerating debates on OPSEC, trust, and the viability of malware-as-a-service (MaaS) within Russian-language forums.

Operation Endgame's impact clarifies which parts of the Russian underground the state is willing to protect and which it is not willing to protect. Russian authorities have conspicuously moved against certain facilitators (for example, Cryptex, UAPS, and later, Aeza-linked executives). At the same time, higher-value ransomware networks with suspected ties or usefulness to security services have largely avoided commensurate consequences, reinforcing our assessment that Russia's "safe haven" is conditional, selective, and governed by state interests rather than law.

Threat Analysis

Russian Government Actions and Response to Operation Endgame

Since the start of Operation Endgame, open-source media, comments in leaked chats, and public posts on various Russian-language criminal sources have indicated that Russian authorities have targeted key services that enable ransomware operations. **Appendix A** shows a timeline of Russian enforcement operations Insikt Group has been monitoring. Based on our review of leaked private communications between threat actors, other arrests likely occurred, but it is unclear whether other non-publicized events exist.

These operations are not merely episodic police work; they are indicators of how the "politics of protection" functions in practice. Actions against facilitators like Cryptex or UAPS — raids, mass detentions, and asset seizures — demonstrate that Moscow will act when services are politically costly or provide limited intelligence value to the state, especially after Western pressure concentrates attention on specific nodes in the ransomware economy. By contrast, comparatively muted or opaque steps against Trickbot-linked figures,

despite European Union (EU) “Most Wanted” designations and extensive Operation Endgame signaling, align with evidence from leaked chats to suggest that ties between senior operators and security services persist. This suggests there is insulation where threat groups retain strategic utility for the state.

This selective pattern matters for three reasons. First, it reframes the “safe haven” idea as conditional: Russia is safest for threat actors who serve state interests, while monetization layers without state value (for example, laundering services) become expendable under pressure. Second, it alters underground behavior. Operation Endgame triggered OPSEC overhauls, forum debates, and trust fractures among affiliates, pushing operators toward closed channels, stricter vetting, and new business models. Third, it clarifies attribution risk for defenders and policymakers; high-value ransomware ecosystems persisting while cash-out infrastructure is dismantled signals that this asymmetry is a result of the state’s cost-benefit calculus instead of a misstep in law enforcement.

In short, the timeline of Russian enforcement following Operation Endgame highlights where Russian threat actors prioritized their resources in response to counter-ransomware efforts. Crackdowns on Cryptex or UAPS and pressure on hosting providers like Aeza demonstrate a willingness to act where domestic optics or Western scrutiny are high, while lenient or performative outcomes (for example, suspended sentences for REvil threat actors) and the continued prominence of Conti and Trickbot alumni reveal where the covenant still holds. This is why documenting both public actions and rumored, unpublicized arrests matters. The mix of visibility, selectivity, and outcome severity maps the contours of protection versus enforcement, and, therefore, where Western disruption is effective and where resilience persists.

Conti: Multiple Layers of Protection Insulate it from Significant Action

As part of Operation Endgame, European authorities persistently targeted Conti Ransomware Group members, affiliates, and close associates, including Trickbot, who enabled their ransomware activities. (Conti and Trickbot are interlinked, as Conti is a ransomware variant developed by members of the Trickbot Gang.) The persistent focus on Conti and Trickbot acknowledges their outsized role as a talent hub, a service marketplace, and, crucially, a network with alleged touchpoints to Russian services.

Operation Endgame included sending targeted videos to the threat actors to receive further intelligence, seizing infrastructure, and publicly naming members of the threat group while adding them to the EU’s Most Wanted list. Operation Endgame’s mix of technical seizures and “naming-and-shaming” was designed to pressure not only operators but also their suppliers and social networks. In Dark Covenant terms, this tactic probed the connection between these criminal enterprises and their state-linked protection: When public attribution raises diplomatic costs, insulated threat actors must either lean more heavily on their protectors or fragment.

As part of Season 1 (2024) in May 2024, the German Bundeskriminalamt (BKA) named Fyodor Aleksandrovich Andreev (aka “Angelo”) to its most wanted list for his role as a member of the Trickbot group. In July 2024, Russian media reported that Andreev had been arrested. Around the same time as the arrest of Andreev, within the leaked BlackBasta chats, Insikt Group uncovered that other members of the Conti Group based in Ukraine had been detained or searched. Also in September 2024, another Conti member

disclosed to “Tramp” that they were released from custody; it is unclear when they had been arrested. However, many of these events targeting Russian Conti or Trickbot members have not been publicized in Russian or English media.

This pattern — sporadic detentions, rapid releases, and sparse official coverage — reads as reputational triage rather than a decisive campaign. Short, ambiguous custodial actions can satisfy external pressure while preserving the threat group’s operational core and its perceived value to state actors. It also creates strategic ambiguity inside the underground: members cannot tell whether arrests signal real risk or performative pressure, which frays trust and complicates affiliate recruitment without dismantling leadership.

As part of the second tranche of Operation Endgame announcements, the German BKA also publicly announced the following additional Conti and Trickbot members had been added to the EU’s Most Wanted list:

- Iskander Rifkatovich Sharafetdinov (aka “alik”, “gucci”), 32, a member of Trickbot
- Mikhail Mikhailovich Tsarev (aka “mango”), 36, a member of Trickbot
- Maksim Sergeevich Galochkin (aka “Bentley”, “Manuel”, “Max17”, “volhvb”, “crypt”), 43, a member of Trickbot
- Vitalii Nikolaevich Kovalev (aka “stern”, “ben”, “Grave”, “Vincent”, “Bentley”, “Bergen”, “Alex Konor”), 36, a member of Trickbot

But despite these additions, Insikt Group has not yet observed Russian law enforcement actions against these individuals. This is likely due to Conti and Trickbot receiving various degrees of protection from multiple groups within the Russian government, ranging from politicians to the security services. In fact, within the BlackBasta leaked chats, “Chuck”, one of the developers of Qakbot, claimed that Bentley, the leader of Trickbot (Vitali Nikolaevich Kovalev), was linked to the Russian Federal Security Service (FSB). German authorities also state that Kovalev was the leader of the Conti Ransomware Group using the moniker “Stern”. However, multiple higher-level members of Conti and its predecessor, Trickbot, likely have links to Russian intelligence beyond Kovalev, including “Professor”, “Target”, “Silver”, and “Brooks”, who openly discuss their relationship with Russian intelligence in other leaked chats.

The juxtaposition is telling: Western warrants escalate transparency and travel risk, while the absence of matching Russian action signals enduring domestic protection. That asymmetry is the essence of the “politics of protection.” If senior figures can rely on connections to intelligence or political patrons, the deterrent effect of international designations diminishes inside Russia. Practically, it allows Conti and Trickbot alumni to preserve leadership, developer pipelines, and affiliate coordination, even as rebrands and splinters create a veneer of churn.

Based on analysis of the leaked Tricktbot and Conti chats, there is anecdotal evidence that Conti (or at least members of it) received some tasking from various unknown Russian intelligence officials. In one instance, Professor provided a list for the Russian GRU to review. Some researchers speculate that this was a list of historical targets supplied to the GRU for further targeting. In addition, Professor was aware that his “paying” SVR contacts were requesting intelligence related to COVID-19. Based on Professor’s comments, it is

implied that either he had an informant relationship with SVR or paid them bribes to ensure they would not be arrested.

Separately, several victims of Conti also align with the interests of Russian Intelligence; this would include Bellingcat and Academi LLC (formerly Blackwater). Conti supposedly targeted the open-source intelligence (OSINT) investigations network members of Bellingcat for the FSB. Based on leaked Conti chats, Conti also conducted a July 2020 breach of the US Private Military Contractor Academi. It is unclear whether this was tasked or whether they were fulfilling some patriotic duty; however, it seems the Russian government did receive files from Academi.

Even if anecdotal, these touchpoints map a spectrum of linkage — tasking, paid relationships, and “patriotic” servicing — that fits Dark Covenant’s direct/indirect/tacit model. For defenders and policymakers, this matters because it blurs the boundary between criminal profit-seeking and state-directed collection. When victim selection overlaps with state priorities, disruption becomes harder; you are not just dismantling a profit engine, you are degrading a potential auxiliary of state intelligence, which is more likely to be sheltered at home and harder to fracture abroad.

Additionally, according to a separate researcher, Conti likely had protection from Vladimir Ivanovich Plotnikov, a member of the Russian Duma from Perm. According to the researcher, Plotnikov was purportedly on several private flights with members of Conti when they went to Dubai in the United Arab Emirates (UAE). Based on this, it is likely that Plotnikov is providing some sort of protection to those who flew with him to the UAE. Figure 1 displays images of Plotnikov from a Telegram channel.

Контрольный выстрел: Conti Leaks

1,989 subscribers

Плотников Владимир Иванович — действующий депутат Государственной Думы РФ от Пермского края и высший криминальный авторитет - "вор в законе"

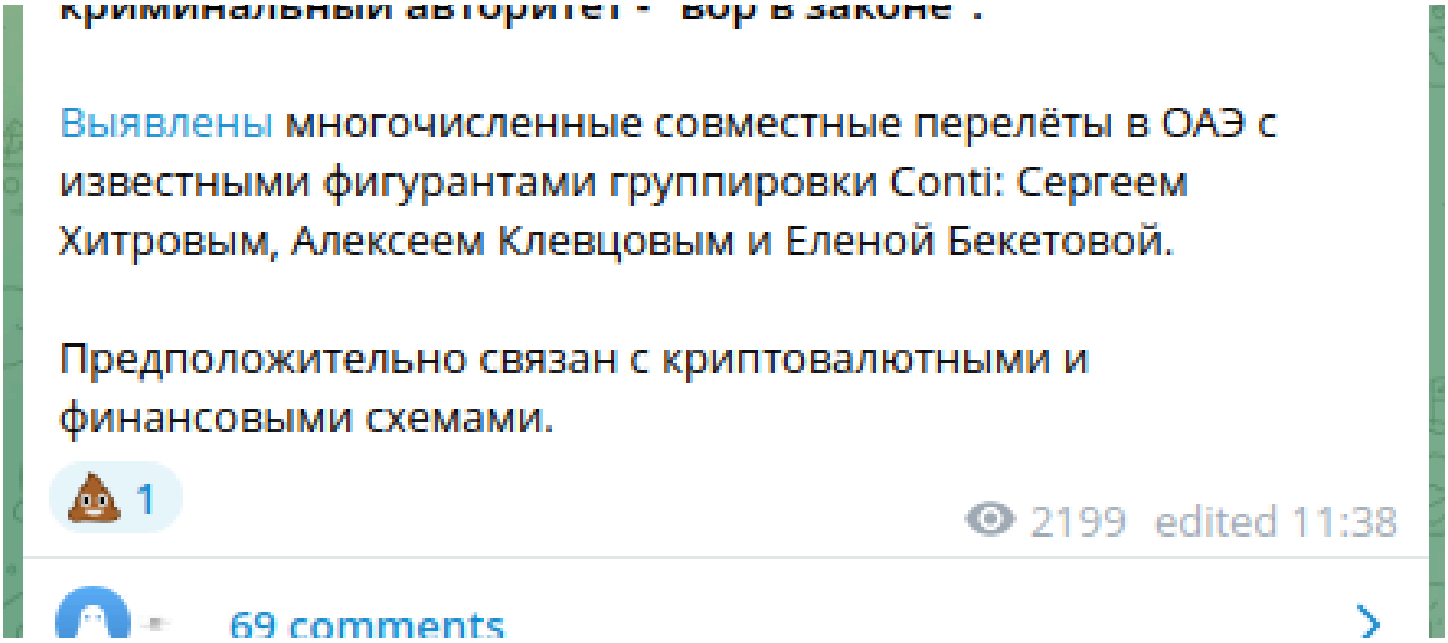

Figure 1: Telegram message highlighting Plotnikov and his relationship with Conti (Source: Recorded Future)

Alleged ties to a sitting Duma member illustrate how protection can extend beyond security services into political patronage networks, broadening the shield available to high-value threat actors. For the underground, such relationships signal who is "untouchable," reinforcing hierarchy and attracting affiliates. For external disruptors, they explain why sanctions, designations, and even arrests abroad may not trigger corresponding domestic action. Political capital at home outweighs reputational costs abroad. In aggregate, these layers — intelligence touchpoints, bribery or "insurance," and political patrons — help explain why Conti- and Trickbot-linked figures have weathered Operation Endgame's pressure better than cash-out services and peripheral enablers.

Cryptex/Taleon Operation Indicate a Worn-Out Relationship

In September 2024, under Operation Endgame, American and European authorities seized infrastructure and cryptocurrency proceeds related to three money laundering services operated by Sergei Ivanov: Cryptex, PM2BTC, and UAPS. In addition, the US Department of the Treasury sanctioned Cryptex and Sergey Ivanov for their roles in laundering proceeds from numerous online illicit services, including ransomware, through these platforms. The Financial Crimes Enforcement Network also named PM2BTC, which does not have a know-your customer (KYC) policy, a primary money laundering concern. The US government alleges these services have been used to launder over a billion dollars in criminal proceeds.

This cluster of actions is significant because it strikes at the monetization layer that underpins the broader ransomware economy. Targeting Cryptex, PM2BTC, and UAPS — then amplifying the pressure with sanctions and a "primary money laundering concern" designation — signals to Russian authorities that specific nodes are now diplomatically costly for the Kremlin to ignore, raising the reputational price of continued tolerance. Furthermore, when trusted laundering schemes are dismantled, affiliates hesitate, deposits and collateral demands rise, and the perceived safety of operating inside Russia narrows, even if core ransomware groups remain insulated.

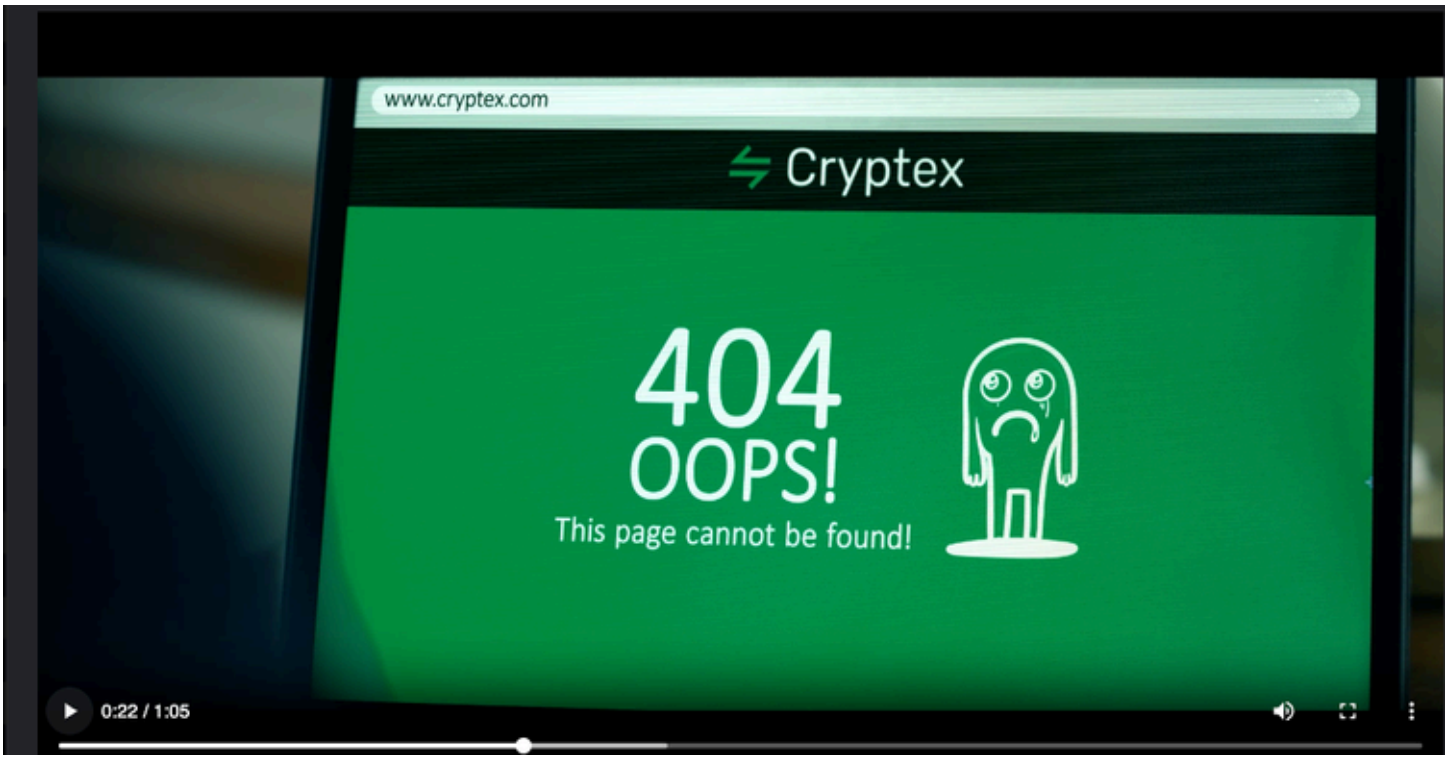

Figure 2: Image from the Operation Endgame video about Cryptex. (Source: operationengame[.]com)

As of October 2, 2024, approximately one week after the UAPS operation, the SKR publicly announced the opening of an investigation into the UAPS payment system and the Cryptex cryptocurrency exchange. As part of this announcement, the SKR claimed to have arrested nearly 100 people associated with these services, seized $16 million in Russian rubles, and also seized various vehicles and property. As of December 2024, at least two members (Ruslan and Roman Orekhovsky) were still under house arrest while the leader of the threat group (Sergey Ivanov) was in pre-trial detention.

The speed and optics of the SKR announcement — mass detentions, cash and property seizures, and highly visible imagery such as the cash-seizure photo (**Figure 3**) — suggest a case chosen to demonstrate domestic responsiveness without touching higher-value, state-useful ransomware networks. The choice of target (financial facilitators rather than core operators) and the lead agency (Investigative Committee rather than security services) align with an equilibrium: money services are expendable when foreign pressure is high and their intelligence value is low, whereas threat groups with alleged service ties retain relative insulation. The legal outcomes to date — house arrest for some, pre-trial detention for Ivanov — preserve prosecutorial theater while leaving room for negotiated resolutions, consistent with past Russian cybercrime cases where sentences are lighter than Western benchmarks. For defenders and policymakers, this asymmetry is instructive, as Western pressure can force action, but Moscow determines how this action will be enforced. It also clarifies where disruption will occur next (for example, hosting providers and payment brokers) versus where resilience will persist (state-linked operator circles).

Screenshot from a video posted by the Investigative Committee of Russia on Oct. 2, 2024, showing large amounts of cash and a money counting machine. (CyberScoop)

Figure 3: Picture of money seized in SKR operation targeting Cryptex and UAPS (Source: CyberScoop via SKR)

The Safe Haven Theory Has Become More Nuanced

Insikt Group assesses that the relationship between Russian cybercriminality and security services is nuanced, as it is affected by multiple variables. This nuance reflects a shifting mix of direct ties, indirect facilitation, and tacit tolerance that varies by threat actor utility to the state. This concept does not account for bribery, Russian services coopting a relationship with cybercriminal actors for a greater benefit to the state, or that rivalries might exist between Russian government agencies. These incentives and rivalries help explain why certain nodes (for example, monetization services) are expendable while core operator circles with perceived intelligence value are insulated.

Based on known incidents, it is most likely that Russian cybercriminals pay security services for protection; these services also likely call on cybercriminals to support the state in the form of data or cyber attacks. This reciprocal arrangement creates a conditional “safe haven” that tightens or loosens depending on political cost, external pressure, and the threat actor’s ongoing usefulness. If the threat actor becomes too significant or does not provide enough support, security services will leverage their legitimate powers to target or harass the victim with their legitimate policing powers. Such episodic enforcement is best read as governance of the market, not its eradication.

However, once it has left the investigative phase, recent sentencing in Russian courts has maintained the appearance of Russia as a haven, for example, despite Russian authorities arresting multiple REvil threat actors in 2023. REvil threat actors have not received similar sentences to what they could receive in the United States (US). According to open-source reporting, Russian courts gave these individuals suspended sentences. This is similar to previous arrests, such as those tied to RBS Worldpay, where suspects received suspended sentences. Lenient outcomes signal to domestic threat actors that as long as there are no targets within Russia and the Commonwealth of Independent States (CIS), they will receive limited punishment for their activities, reinforcing the covenant's credibility despite headline arrests.

Insikt Group assesses that, at least in some instances, Russian authorities were likely aware of these threat actors and took action only because of Western pressure. This aligns with a "pressure-response" pattern in which Moscow prioritizes reputational management over dismantling strategically useful networks. The threat actors were not providing something of value to the state compared to the pressure being placed on Russian authorities. For example, with Cryptex, Russian authorities initiated an investigation, identified over 100 subjects, and developed a cause within their legal regime to arrest them. In addition, the courts determined that Sergey Ivanov should stay in detention as of December 2024. The lead investigating agency was the Investigative Committee, rather than the Ministry of Internal Affairs or the FSB. Regardless of investigative agency, this timeframe seems impractical for such a complex multi-region operation, indicating that this threat actor was likely tracked for some time before the operation. This is also reflected in public posts on criminal forums, where one threat actor said that Cryptex had to have been under surveillance of Russian authorities for a period of time for this to have occurred. Taken together, these factors suggest the operation was a prepositioned lever — activated when international costs rose — rather than a spontaneous crackdown.

Within Russian-speaking cybercriminal sources, there were minimal public posts on the matter. Several threat actors on Korovka Forum showed dismay and surprise that Russian law enforcement acted in general. Several Verified Forum threat actors also hesitated to use services similar to Cryptex and forums in light of the recent actions. This chilling effect on cash-out services illustrates how targeted pressure reshapes underground risk calculus even when core ransomware operators remain intact.

The targeting of Ivanov and Cryptex could be due to which agency conducted the operation, or because Ivanov and Cryptex were solely related to money rather than providing information and data to Russian authorities. That distinction — money versus intelligence utility — is central to where protection is extended or withdrawn. Some members of Conti had intimated that the Intelligence Services were neutral or sympathetic to ransomware operations, while the police (like the SKR or MVD) were on the same side as American services (this was around the same time as there was limited cooperation between Russia and the US post-ransomware attack on Colonial Pipeline in 2021). This split helps reconcile the simultaneous tolerance of operators and pressure on facilitators.

In contrast, Insikt Group has only seen limited operational activity within Russia targeting members of Conti (and its multiple splinter groups), and much of this activity appears to be perceived harassment or intimidation by various authorities. Harassment without decisive prosecutions preserves leverage over threat actors while avoiding the strategic loss of a useful proxy capability. Based on leaked chats and public posts

on criminal sources, Insikt Group has identified Tinker, Bio, and Angelo as having experienced some interactions with Russian authorities. However, Kovalev, the head of Conti, was known to Russian security services. In addition, other members were associated with Russian Intelligence Services; Conti members openly shared information with the Intelligence Services to fulfill intelligence requirements, likely providing the Russian government more utility than money laundering organizations. This asymmetry of treatment is a defining feature of the covenant's "politics of protection."

Within Russian criminal sources, much of the discussion on arrests related to Conti and Trickbot was limited to discussions of how Russian authorities became aware of Angelo and the role of Interpol in the arrest of Angelo. The narrow focus underscores that community concern centers on exposure pathways, not on a fundamental expectation that high-value operators will face severe domestic penalties.

Impact on Cybercriminal Trust and Recruitment

Against this backdrop of selective protection and targeted sacrifices, the market signals inside the underground shifted in ways that map directly to the Dark Covenant's incentives structure and risk calculus.

Since the beginning of Operation Endgame (May 2024), Insikt Group has observed a decrease in the number of open RaaS affiliate program advertisements on the dark web, especially related to long-active and credible ransomware groups. However, the number of new RaaS advertisements was still significant — we have seen at least 21 open RaaS affiliate programs launched since May 2024. The primary platforms for advertisements were Ramp, XSS, BreachForums 2, and Telegram. For the same period, we observed that in addition to Commonwealth of Independent States (CIS) countries, ransomware operators block any attacks on BRICS countries (China, India, Brazil, South Africa, Russia, Egypt, Ethiopia, Indonesia, Saudi Arabia, and the UAE). Ransomware operators still prefer Russian-speaking affiliate members over English-speaking ones because they assess that the English-speakers are more likely to be researchers or Western law enforcement agents who can pose a significant risk to them.

Fewer open advertisements and a pivot toward semi-closed recruitment are rational adaptations to perceived infiltration and selective domestic enforcement. Operators try to keep the revenue engine running while shrinking their exposure surface. The continued emergence of new programs, despite headline pressure, shows the underlying business remains attractive, but the bar for trust is higher and more culturally gated. The explicit "no-attack" carve-outs for BRICS mirror the political boundaries of protection: avoiding blowback against states viewed as friendly or strategically important reduces the chance of losing domestic cover. Finally, the preference for Russian-speaking affiliates is both an OPSEC filter and a social signal, privileging the in-group that is most legible to protectors and least likely to invite Western attention, thereby reinforcing how market behavior and state tolerance coevolve within the Dark Covenant.

Affiliate Member Recruitment or Vetting

For the research period, we did not observe any significant changes in ransomware affiliate member recruitment and vetting processes. They are aligned with the previous requirements; however, since Operation Endgame, we have observed that many ransomware owners have become more selective about

hiring affiliate members. The core mechanics remain intact, but the threshold for entry has risen. Post-Operation Endgame, operators price-in higher detection risk by shrinking the attack surface — favoring known circles, screening harder, and externalizing risk to affiliates — rather than restructuring the RaaS model itself.

- RaaS operators require activities from affiliate members. Typically, they ban affiliate members who have been inactive for one month and delete their accounts. In some cases, the accounts can be banned after ten days (Mamona RaaS) or fourteen days of inactivity (PlayBoy RaaS). Activity requirements function as a trust-and-liquidity control: they weed out sleepers (including potential infiltrators) and keep the pipeline producing ransom leverage, effectively taxing affiliates with “proof of life” to remain inside the circle.
- For security reasons, new affiliate members may be required to make deposits (for example, $5,000) on other reputable forums. Deposits substitute for eroded social capital. Where vouching used to suffice, capital-at-risk becomes the screening proxy, raising costs for scammers and making infiltration more expensive.
- Some ransomware operators do not allow targeting (encrypting and exfiltrating data) of non-profit organizations, healthcare, and government entities (for example, Anubis or PlayBoy ransomware). Targeting rules are both reputational hedges and political boundary markers. They reduce heat from domestically sensitive classes and align with the covenant’s implicit “lines not to cross” that would jeopardize tolerance.
- There is a minimum ransom demand per victim ($50,000 or more). Floor pricing narrows churn, prioritizes higher-yield victims, and preserves brand leverage, compensating for fewer open affiliates by pushing margins up where risk is justified.
- Repeated attacks on the same victims are forbidden. Anti-collision policies protect negotiation credibility and reduce noise that draws attention from law enforcement and platforms — an internal norm that sustains the business under scrutiny.

The above-mentioned restrictions were likely put in place due to the frequent scam attempts and a number of unqualified RaaS affiliate members. On August 11 and 12, 2025, the threat actor “MikeMelton”, a member of CHAOS Ransomware Group, on the forum Ramp, posted that previously, this kind of forum was a privileged place to conduct business and required a perfect reputation and vouching from other credible dark web community members. However, recently, businesses such as hacking and carding started attracting a lot of unskilled and inexperienced individuals or agents, which makes all business threads immediately public; that is why members stopped sharing their experience. It is currently a place for trade and scammers. According to the threat actor, the reputation is based only on a deposit on forums, but not on real activity. This lament captures the structural shift: reputational gatekeeping has degraded under pressure, so markets default to financial collateral and closed-channel vetting. In Dark Covenant terms, as state tolerance grows more conditional and external pressure rises, underground threat actors self-regulate with higher costs and tighter circles, thus sacrificing openness for survivability.

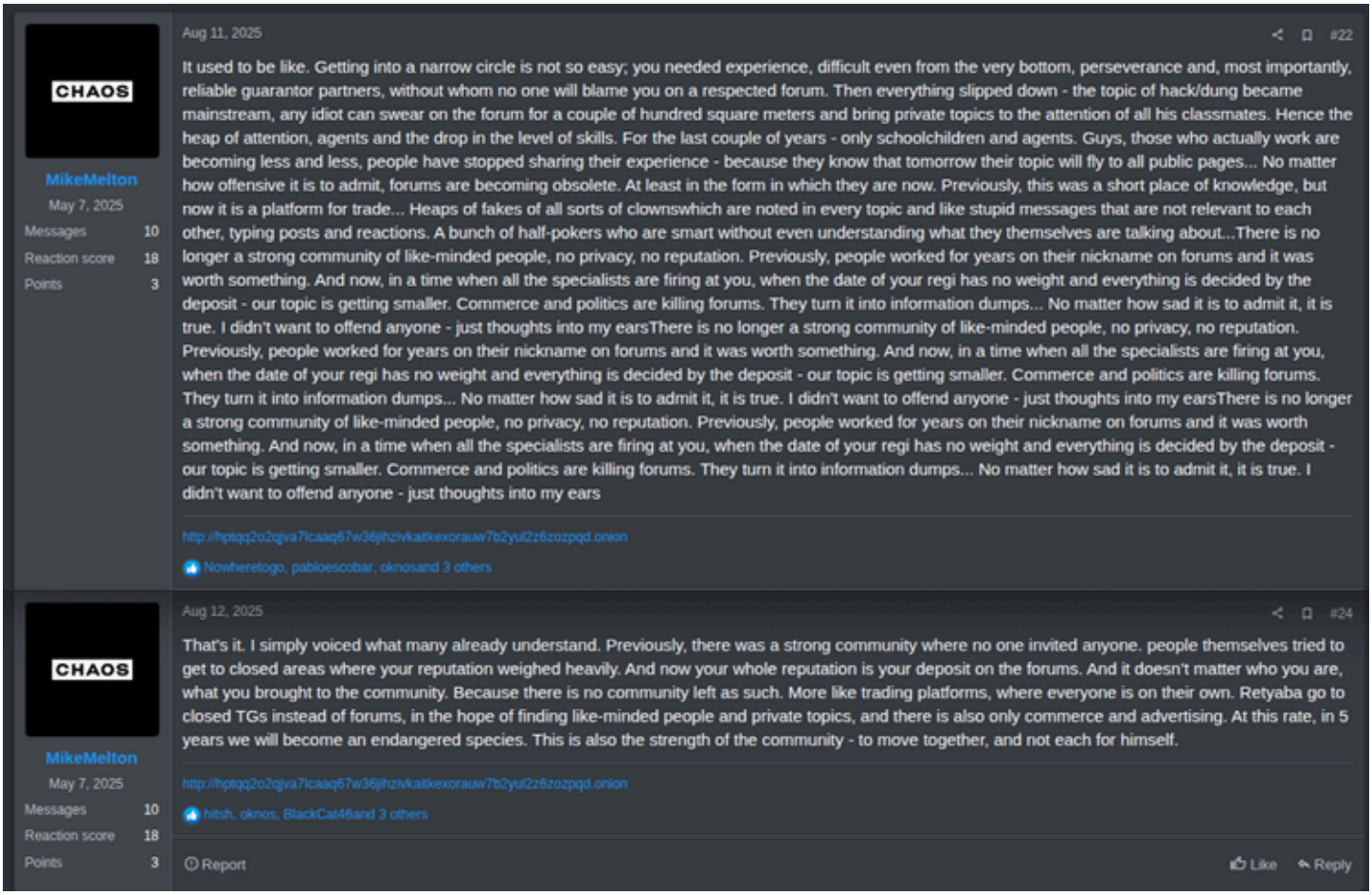

Figure 4: MikeMelton posted their opinion regarding the current dark web community reputations and developments; the post was translated using Google Translate (Source: Ramp Forum)

Examples of Increase or Decrease in Trust Among RaaS Affiliate Members

Since 2024, we have observed posts on dark web forums where threat actors complained about participating in RaaS affiliate programs, stating that ransomware owners scammed them. This erosion of trust reinforces the shift from open advertisements to closed, collateralized recruitment consistent with the covenant's self-protective logic.

Qilin RaaS Affiliate Member Dispute

On July 22, 2025, the threat actor "hastalamuerte" on the forum Ramp filed a complaint against "Haise", an operator and representative of Qilin Ransomware Group on criminal sources. hastalamuerte accused Haise of not paying them their portion of the ransom. The threat actor stated that their team was affiliated with Qilin Ransomware Group and that they targeted fourteen victims within the last one-and-a-half months. They stated that they had an agreement with Qilin Ransomware Group to receive $200,000 for these victims, but the support of Qilin suddenly disappeared, and hastalamuerte estimated a loss in profit of $48,000. This kind of public non-payment dispute erodes the perceived reliability of RaaS "platforms," pushing operators toward tighter, collateralized, and culturally gated affiliate models consistent with the covenant's self-protective logic.

In response to the claim, Haise replied that hastalamuerte is affiliated with “DevManager” (threat actor “Devman”), who tried to work with Qilin and provided corporate networks. According to Haise, Devman has been publishing these victims before closing negotiations on their own extortion website, Devman Blog. Furthermore, Devman allegedly tried to steal the source code of Qilin ransomware and hire one of its developers. They also mentioned another “weird” affiliate member who targeted twenty entities and refused to publish them on Qilin’s extortion blog. hastalamuerte replied that they became a ransomware affiliate through a college of Devman and did not hide that they knew each other. The dispute was closed by the administration of Ramp Forum on July 31, 2025, without any negative consequences for Haise. Forum arbitration that favors the operator over the affiliate signals power asymmetry inside RaaS ecosystems and deters future whistleblowing, but it also accelerates the affiliate flight risk that operators then counter with deposits, KYC-lite checks, and closed recruitment.

The conflicts between affiliate members and RaaS owners happened earlier. Among the most notable examples was the conflict between the currently disbanded ransomware group ALPHV and their former affiliate “notchy”.

Emergence of Ransomware Impersonators

In the second half of 2024 and in 2025, Insikt Group observed multiple instances of the emergence of ransomware group impersonators with pure scam intentions. Among these groups were RebornVC, Babuk 2.0, Bjorka Spirit (Ransomware), GD LockerSec, FunkSec, Dispossessor, and Rabbit Hole. The proliferation of impersonators dilutes brand credibility across the ecosystem, accelerates “trust flight” to closed circles, and raises acquisition costs for legitimate affiliates — outcomes that align with the Dark Covenant’s shift from open markets to tightly managed, state-tolerated networks.

For example, on January 26, 2025, Babuk ransomware v. 2.0 was released on the dark web and included an announcement for their affiliate program. The threat group released the primary terms and conditions of the program, indicating the threat group does not target hospitals (except private plastic surgeries and dental clinics), any non-profit charitable foundations, schools (except major universities), or small businesses (companies with less than $4 million in annual revenue). It is worth mentioning that analysis of the victims posted on the extortion website revealed that 90% of the victims had already been listed by other ransomware groups. According to GuidePoint’s Research and Intelligence Team (GRIT), out of 64 victims initially listed by the ransomware operators on the extortion website, 26 victims had been listed by FunkSec Group, 26 victims by RansomHub Ransomware Group, and four by LockBit 3.0 Ransomware Group. Recycled victim lists suggest opportunistic “signal hijacking,” eroding the informational value of leak websites and undermining extortion leverage — another force pushing operators toward curated channels and vetted partnerships.

In January 2025, Babuk 2.0 ransomware operators announced their cooperation with the threat actor “Bjorka” (same time as GD LockerSec Ransomware Group). These fluid “partnership” claims function as reputational arbitrage: impersonators borrow brand equity to lure affiliates and victims, while real operators respond by tightening verification and provenance checks. Almost immediately in January 2025, Insikt Group observed an increase in Telegram activities associated with “Bjorka Spirit (Ransomware)”, a purported

ransomware group that is operated by the threat actor Bjorka. We assess that Bjorka does not operate a ransomware group, but performs hacking and data leak activities; however, the Telegram group indicates active cooperation between Bjorka and ransomware group operators such as Babuk Locker 2.0, GD Locker, FunkSec, and more.

Insikt Group identified further discussions on the dark web regarding the threat actor “SkyWave”, an alleged member of Babuk 2.0 Ransomware Group, where users claimed that the monikers SkyWave, “Bjorkanism”, and “BabukLocker” are all used by the same individual, Aditya Dani Herlambang. Aditya was born on March 17, 2009, is male, and possibly located in Pangkot, Manado Sulawesi Utara, Indonesia.

We assess that all these threat groups are operated by the same cybercriminal team that constantly publishes already leaked data on the dark web. Telegram banned multiple Telegram channels operated by the above-mentioned groups due to the violation of its Terms of Service (ToS); however, Telegram’s low-entry barriers enable rapid rebranding and audience capture, which inflates noise and further incentivizes serious threat actors to migrate negotiations off public channels.

From May 2024, Insikt Group observed more examples of ransomware and data extortion groups publishing or reselling already compromised data, such as the currently defunct Dispossessor Ransomware Group (primarily reposting LockBit 3.0’s victims) and Rabbit Hole Blog (reselling already leaked data from various ransomware groups). Impersonation and resale schemes are market noise that strengthens the case for smaller, protected constellations of threat actors — those most likely to be legible to domestic protectors and least exposed to Western pressure.

Internal Perception and Community Discussion

Operational Security Discussion

Throughout both the 2024 and 2025 iterations of Operation Endgame, Insikt Group has observed numerous threads on high-tier forums such as Exploit and XSS discussing the takedowns and arrests, particularly with regard to law enforcement deanonymization techniques, recommended operational security changes, and risk calculus for participating in MaaS projects. Insikt Group observed users increasingly urging each other to move to decentralized messaging platforms, citing that centralized communications platforms and email providers comply with law enforcement. Multiple users recommended moving communications from Telegram to platforms such as Session, Jabber, and Tox, though numerous users also cited vulnerabilities in Tox, such as IP address leaking between users. Insikt Group also observed several threads discussing the security of the Tor browser, with one thread expressing skepticism about updates to the browser, Whonix, and Qubes, and other guides published regarding how to use the browser safely. Many users recommend a multi-layer approach to operational security, including the use of Tails, virtual machines, Tor browser, and neighbors’ Wi-Fi networks rather than one’s own. We also observed threads specifically posing the question of protecting data on computers and mobile phones in the case of seizure by law enforcement, with multiple users suggesting the use of VeraCrypt hidden volumes to secure hard drives. Users also compared the security of various mobile operating systems and manufacturers’ willingness to unlock seized devices, with most users agreeing that trusting iOS and Android should be avoided, and several users recommending

GrapheneOS instead, with still others dismissing having a smartphone at all as being insecure and insisting on using older burner phones only.

Analytically, this OPSEC pivot reflects the Dark Covenant in practice: when state tolerance becomes conditional and Western pressure rises, threat actors reduce centralized exposure, raise the technical bar to entry, and privilege in-group channels, trading scale for survivability. These adaptations increase transaction costs for affiliates (deposits, vetting, and toolchains) and fragment visibility for defenders, but they also create new error surfaces (misconfigured Tox, Tor hygiene lapses, and burner OPSEC) that can be exploited. The net effect is a shift from mass, open coordination toward smaller, semi-closed constellations that are more legible to domestic protectors and harder for outsiders to infiltrate.

Concurrent to Operation Endgame, Russian law enforcement engaged in arrests of various ransomware threat actors, including those related to REvil. Within the leaked BlackBasta chats, one of the group members highlighted a REvil-related arrest that occurred in November 2023. As a result, the threat group wiped the wallets and other data they had shared with the arrested REvil threat actor, indicating some fear of further Russian law enforcement actions. This reaction underscores the covenant's "governed market" dynamic: selective domestic pressure is credible enough to compel precautionary hygiene (wallet purges and compartmentation) without dismantling core ecosystems, reinforcing a conditional safe haven that Moscow can tighten or loosen to manage risk and influence behavior.

Lumma Disruption Discussion

In another thread discussing Operation Endgame, which resulted in the takedown of Lumma Stealer infrastructure, multiple users expressed uncertainty in the security of the MaaS model, citing that the operation was openly targeting Lumma affiliates and customers, rather than only the developers and operators of the malware. Multiple users stated that the only way to operate is to write your own stealers and malware and store your own data privately, stating that users should not trust "public" commodity malware providers like Lumma. The user "Theriella" stated that Lumma developers are likely safe due to their presence in Russia, and that although this likely means that they need to give a cut to the "structures" (likely institutions such as law enforcement), it was still better than operating on US territories; another user countered by saying that eventually "money will run out and your own will eat you to the bone." This debate captures the Dark Covenant tradeoff: commodity MaaS maximizes scale but invites cross-border exposure, while "write-your-own, keep-your-own-data" models shrink visibility and re-center protection on domestic ties — especially if developers can "tax" themselves to local structures for cover. The perception that Russia-based developers are safer, even if they share proceeds with "structures," reinforces a governed-market logic in which proximity to protectors substitutes for platform trust.

Several users also claimed that despite the disruption, Lumma "went private" via closed channels, which aligned with observations from researchers of continued infections and log availability. Notably, as of September 2025, Lumma has appeared to resume public-facing operations with an August 29, 2025, post on Ramp Forum releasing updates to Lumma, with inclusion of a link tree (usrlnk[.]io/lumma) as well as a Telegram handle ([@]lummaseller128) for purchasing access to the panel. This oscillation, from public to private and back, illustrates resilience patterns common in covenant-aligned ecosystems: close ranks under

pressure, monetize quietly while the situation is intense, then re-emerge when enforcement attention shifts. For defenders, it implies that takedowns depress liquidity temporarily but do not eliminate capability; for policymakers, it signals that durable impact requires sustained pressure on both operators and the domestic incentives that enable their return.

Discussions of Charged Individuals

In addition to analyzing individual threads, Insikt also tracked user activities of individuals implicated in Operation Endgame and discussions of their forum activities. We observed that several users named by the operation, such as “Jimmbee” (Aleksandr Stepanov), “psevdo”, and Chuck, remain members of their respective forums and have not been banned by administrators. Other users, such as the developer of Lumma (“Shamel”), were banned on the forum per their own request. The continued presence of named users, absent universal bans, signals that underground governance prioritizes utility and reputation over external designations, reinforcing the covenant’s logic that social capital and perceived protection can offset public exposure.

Users on Exploit and XSS forums also shared their thoughts regarding the fate of individuals named and arrested in the campaigns. In a thread about the DanaBot takedown and arrests during Operation Endgame, user Theriella wrote about the possibility of suspects being recruited by either the American or Russian government, claiming that in the latter case, they will be “forced to work for the government in a golden cage with a collar.” This “golden cage” narrative aligns with Dark Covenant dynamics: selective coercion converts high-skill criminals into semi-deniable assets, preserving capability while tightening state leverage. The same thread discussed operational security mistakes that arose as a result of a memory leak vulnerability in DanaBot code itself, which leaked threat actor usernames, IP addresses, command-and-control (C2) infrastructure domains and addresses, private keys, and more. In a separate XSS thread discussing the 2024 operation, users analyzed Operation Endgame’s videos posted to the takedown website, discussing which usernames are linked to an individual, or theorizing about what law enforcement knows about various individuals and who is a “rat” that led to the arrests.

Attribution speculation and “rat” hunting fragment trust and push threat actors toward tighter compartmentation, consistent with the shift from open forums to curated circles. Another user, “Asist”, commented that the account associated with SmokeLoader (“SmokeLdr”) should be banned for security reasons, though as of September 2025, the account remains on the forum. The reluctance to ban legacy brands underscores the weight of reputation and revenue potential even amid security concerns.

Discussions of the law enforcement operations themselves also seemed to spur more existential discussions on the forums around the cost-benefit analysis of engaging in financially motivated cybercrime at all. In one thread on Exploit Forum, the user “RichAsHell” commented on the difficulty of netting high profits via cybercriminal activity, particularly for those just starting out, stating that the risk of decades in prison makes working in “white” (non-criminal enterprise) to make comparable profits more appealing. This reevaluation reflects rising transaction costs (deposits, stricter vetting, closed channels) and elevated perceived risk — clear downstream effects of Operation Endgame and conditional domestic enforcement. The topic was controversial among Exploit users, with some claiming that cybercrime was more profitable than any “white”

work in former CIS countries, or other financially struggling economies such as those in Africa and Southeast Asia, especially outside of major cities.

Economic grievance narratives help sustain recruitment despite higher risk, but they also push operators to professionalize and centralize control over who participates. The user “Ex0rci$t” commented that at the inception of Exploit, there was no criminal punishment for carding within the Criminal Code of the Russian Federation, citing the uncertainty around further criminalization of forum activities within Russia. This legal uncertainty is a feature of the covenanted space: ambiguity preserves state flexibility to pressure or protect as needed, maintaining leverage over the market while avoiding categorical commitments.

Transnational Policy Changes in a Post-Operation Endgame Environment

Western governments continue to evolve in their policies toward ransomware, mainly taking a proactive stance and implementing disclosure guidelines so that law enforcement and governments can actually measure the ransomware threat. This shifts the external environment from episodic disruption to continuous measurement and pressure, raising the cost of doing business for Russia-based ecosystems while illuminating where domestic protection sustains activity despite exposure.

While this is happening, the US and Russia have engaged in diplomatic efforts that have resulted in the release of multiple sentenced Russian cybercriminal threat actors (Alexandr Vinnik, Roman Seleznev, and Vladislav Klyushin), which might imply that if an incarcerated threat actor is significant enough, they can weigh this as an option in their negotiations. Klyushin and Seleznev were released in August 2024 as part of a multinational exchange. Klyushin had been arrested for his role in a securities scheme where Klyushin and others hacked into computer networks to steal confidential corporate information that was used to make $93 million in profits through the stock market. Klyushin was likely released due to his company’s contracts with the Kremlin and one of his codefendants being a GRU officer who was involved in hacking the Democratic National Committee in 2016. Roman Seleznev, who was associated with various hacking and payment card fraud schemes, was likely released because he is the son of Russian Duma member Valery Seleznev. Alexander Vinnik was released in February 2025 and had pleaded guilty to laundering billions of dollars in cryptocurrency. Prior to Vinnik’s arrival back in Russia, the Russian Ministry of Internal Affairs had its own investigation to stop his extradition to the US. Due to the prisoner exchange, Russia removed the criminal case against him, and he was freed upon his return to Russia. These swaps underscore how high-value threat actors function as geopolitical assets; the possibility of exchange or protection reduces deterrence for elites and reinforces the covenant’s logic that proximity to state power can offset foreign legal risk.

Since the beginning of Operation Endgame, multiple ransomware attacks originating from Russia continued targeting Western entities, which forced the governments of many countries to reassess their approach toward ransomware payments, negotiations with ransomware operators, reporting procedures, and identifying key adversaries. Below is a list of the major legislative changes for the past years in the US and in some other highly targeted countries. In 2025, the US signed two presidential orders (1, 2) to reinforce the cybersecurity posture that protects the US’s internet and telecommunications infrastructure. The law also allows the US government to take more effective actions against state-sponsored cyberattacks orchestrated by the governments of Russia, China, Iran, and North Korea, and implies the development of minimum

cybersecurity standards for government technology contractors with a primary focus on China. By formalizing authorities and standards, Western states are narrowing the gray space in which state-tolerated criminal actors operate, making it harder for Russia-based threat groups to rely solely on domestic protection while transacting internationally.

In addition, Japan is moving to a more offensive cyber approach. On May 16, 2025, Japan implemented a new Active Cyberdefense Law that permits the authorities of Japan to perform offensive cyber operations regarding hostile infrastructure and adversaries, including infiltrating and neutralizing hostile servers before any malicious activity has taken place, and decreasing the level of attacks on Japan. This normalization of preemptive action signals that the external pressure on Russia-based ecosystems will include active defense — not just post-incident cleanup — compressing the operational windows the covenant seeks to preserve.

- On May 31, 2025, Australia began enforcing new ransomware payment disclosure rules under the Cyber Security Bill 2024, requiring businesses with an annual revenue above $3 million AUD (USD $1.92 million) to report any ransom payments to the Australian Signals Directorate (ASD) within 72 hours. This legislation, while not making ransom payments illegal, mandates transparency to enhance the government's insight into ransomware activity and inform future cybercrime legislation. Companies must report details such as their Australian Business Number, timing of the attack, whether data was stolen or encrypted, vulnerabilities exploited, the ransom amount and currency, and the financial impact on the business.
- On January 14, 2025, the UK government initiated an open consultation called "Ransomware: proposals to increase incident reporting and reduce payments to criminals" with a proposed launch date of April 8, 2025. According to the proposal, regarding a ban on all public sector bodies, including schools, the National Health Service (NHS), operators of Critical National Infrastructure (CNI), and local councils, from making ransomware payments. The proposals also include mandatory reporting of ransomware incidents, aiming to enhance transparency and improve response strategies. Previously, UK government departments were banned from paying ransoms to ransomware operators. That process is a part of the broader strategy to combat cybercrime and minimize the risk of financial losses and other damages to businesses and infrastructure. As of this writing, the legislation has not been implemented yet, but the published government response demonstrates a strong intention to proceed further with legislation in the foreseeable future.

Payment visibility and bans reduce liquidity for RaaS ecosystems, raise negotiation risk, and weaken extortion leverage. This constrains the monetization channel that domestic protection alone cannot guarantee, pressuring Russia-based threat actors to adapt or lose profitability.

Operational Adaptations by Russian Cybercriminals

Throughout 2024 and 2025, Insikt Group has observed that Russian domestic policies and enforcement strategies have contributed to threat activity enablers' (TAE) operational adaptations following sanctions and enforcement activities. Historically, such providers have operated with relative impunity due to weak domestic enforcement; however, the April 2025 arrests of Aeza Group executives Yuri Bozoyan, Maxim Orel,

and Tatyana Zubova marked a departure from this trend. These arrests were linked to Aeza's hosting of the darknet drug market BlackSprut, which had previously gained high visibility through public billboards in Moscow. This was a boundary enforcement event: when criminal infrastructure drifts into politically sensitive domains (domestic narcotics and public optics), tolerance narrows and the state signals costs — even if adjacent cyber or influence operations remain tolerated.

The Aeza arrests were followed by a considerable loss of trust in the provider within the cybercriminal ecosystem, with multiple user complaints about downtime and payment suspensions surfacing on forums such as LolzTeam (which resulted in bans). Multiple other Russian TAEs, such as CloudBlast and VDSina, moved quickly to fill the vacuum left by Aeza, offering targeted "refugee services." Additionally, the Western government announced sanctions against Aeza in July 2025, leading Aeza to adopt a dual structure: the company migrated its infrastructure to Serbian provider Smart Digital Ideas DOO while continuing to rely on Russian financial systems such as WebMoney, YooMoney, and Mir for payments.

We assess that this likely reflects an attempt by Aeza to balance operations between enforcement strategies inflicted by both Western governments and Russian domestic law enforcement. Notably, Aeza had also been linked to hosting the pro-Kremlin disinformation campaign Doppelgänger, active in Europe since at least 2022. This indicates that while Russian authorities may tolerate and even use hosting services tied to cybercrime or disinformation, direct association with domestic narcotics distribution introduced political sensitivity that triggered intervention. The "dual structure" response is a typical covenant adaptation: externalize exposure (infrastructure migration abroad) while anchoring monetization at home, preserving access to domestic protection and payments, even as reputational and regulatory pressure increases.

On the other hand, TAEs such as Stark Industries, Global Connectivity Solutions, Inferno Solutions (3NT), and Zservers demonstrated different adaptations in response to Western sanctions. Stark Industries pre-emptively migrated its Russian infrastructure to Moscow-based UFO Hosting in advance of EU sanctions, likely to ensure continuity for both domestic and international clients. Global Connectivity Solutions and Inferno Solutions have also maintained stronger domestic ties, continuing to use long-standing networks while insulating their operations through UK-registered fronts. Their resilience is supported by the domestic reality that Russian authorities have not targeted them, given their role in state-aligned disinformation and cyber operations rather than domestic narcotics markets. Stark Industries was also reportedly cooperative with Western law enforcement in Operation Endgame, with cybersecurity company Cymru claiming that PQ Hosting/Stark Industries was a "key partner and collaborator" in the takedown (the company has historically been observed to selectively cooperate with law enforcement requests, likely further contributing to their resilience). These heterogeneous strategies — preemptive repositioning, foreign façades, and selective cooperation — illustrate how TAEs navigate the covenant's incentives. They remain useful to state priorities, avoid domestically sensitive red lines, and trade limited cooperation for operational continuity.

Ransomware Adapts and Grows Despite External Pressure

The primary trends Insikt Group observed since the beginning of Operation Endgame can be divided into two groups: those that continued to evolve from the previous report's timeframe and new trends that significantly changed the ransomware threat landscape. These trends reflect a market seeking volume and

dispersion to offset enforcement, while concentrating trust and protection where domestic cover is strongest. Among the primary evolution trends were the following:

First, a stable growth in the number of new ransomware variants. For example, from May to December 2024, we identified at least 192 new ransomware variants. From January to September 2025, the number of new variants was 236. The majority of the variants originated from leaked source code and builders from existing ransomware families such as LockBit, CryLock, Xorist, Proton, GlobeImposter, Chaos, Makop, MedusaLocker, Djvu, Dharma, and more. We assess that this trend will continue and increase in volume. The launch of a new ransomware variant can and often does garner media attention, something that a threat actor or group may want at times. As threat groups gain knowledge in developing and deploying their own ransomware variants via leaked data, they will likely add this attack vector type to their TTPs. In some cases, Insikt Group observed that allegedly different ransomware variants used identical methods of communication, which indicates these threat actors have low credibility. Proliferation via leaked builders spreads capability without deep benches or protection, producing noisy “brands” that chase attention but lack credibility — an ecosystem-level adaptation that raises defenders’ triage burden while leaving core, protected crews comparatively insulated. To name a few examples:

- Root ransomware, Foxtrot ransomware, and Pomochit ransomware used identical email addresses (pomocit01@kanzensei[.]top and pomocit01@surakshaguardian[.]com).
- Destroy ransomware and AttackNew ransomware used identical email addresses (ithelp01@securitymy[.]name and ithelp01@yousheltered[.]com).

Second, there has been a stable growth of new ransomware extortion websites. For example, from May 2024 to December 2024, Insikt Group identified 34 extortion websites, and from January 2025 to September 2025, 60 extortion blogs. More blogs diversify pressure channels and complicate takedowns but also fragment trust; serious operators respond by steering negotiations to curated venues, reinforcing closed-circle dynamics consistent with the covenant. Not all ransomware variants operate their own extortion blogs. Insikt Group assesses that it is relatively easy to create and deploy a new variant, but there is a bottleneck as to whether the variant is actually successful enough to obtain victim data for launching an extortion website.

Third, ransomware focus has turned toward Asian countries. In 2024, India was the most targeted country in Asia and number seven in the world, with 100 listed victims on extortion websites. In June 2025, Israel became number four among the most targeted countries worldwide. However, it is likely that Israel was targeted more frequently than usual this month due to the conflict with Iran, which spurred a wave of opportunistic attacks by various cybercriminals. Shifts in geography reflect opportunism and political risk management: threat actors pursue high-yield targets while avoiding jurisdictions that threaten domestic protection or trigger disproportionate response.

Fourth, new ransomware groups continue using pressure tactics to extort victims, such as distributed denial-of-service (DDoS) attacks or phone calls to victims to threaten them to pay ransom. These new RaaS groups will also continue hiring affiliate members openly, primarily via their extortion blogs or Telegram channels or forums, specifically Ramp Forum. Escalation tactics substitute for waning payment rates; open hiring

persists at the edge of the market, while established brands tighten gates — dual tracks that balance volume with survivability.

Fifth, operators of ransomware variants based on leaked source codes of notable ransomware brands widely adopted another pressure method: double ransom payments unless a victim pays a ransom within 24, 48, or 72 hours after a ransomware attack. Time-based penalties aim to compress negotiation windows before law-enforcement and regulatory friction can intervene, acknowledging a more hostile external environment.

Sixth, existing ransomware groups continued to rebrand for security reasons. Rebranding serves as a reputational reset and legal smokescreen, enabling protected cores to shed heat while retaining talent, infrastructure, and state-aligned utility within the covenant's protective boundaries.

Changes in Ransomware TTPs

Since May 2024, Insikt Group has observed different approaches in the business model of RaaS operators and changing TTPs. New approaches we observed are outlined in **Appendix B**.

Increase in Rivalries Between Ransomware Groups

Dragon Force, RansomBay, and RansomHub Conflict

In April 2025, Insikt Group identified that Dragon Force Ransomware Group announced several controversial statements regarding its project "DragonBay" and RansomHub Ransomware Group on the forum Ramp:

- On April 1, 2025, it was noticed that RansomHub Ransomware Group went offline and stopped operations. Some researchers stated that at least part of the threat group likely migrated to Qilin RaaS since the number of its victims almost doubled since February 2025. Qilin Ransomware Group was observed advertising a new RaaS version and hiring more affiliate members.
- Almost simultaneously, on April 2, 2025, the threat actor dragonforce released a statement that indicates that RansomHub likely joined their infrastructure and started cooperating.

On April 25, 2025, dragonforce denied any attacks against RansomHub Ransomware Group on Ramp Forum. However, on April 28, 2025, the threat actor "koley", a member of RansomHub Ransomware Group, claimed that Dragon Force Ransomware Group was responsible for the attack against RansomHub's infrastructure and disruption to its operations. Also, they stated that they identified a traitor within RansomHub, an individual with the moniker "sarg0n" (possibly sarg0n, a member of Exploit and XSS forums) whose alleged name is "Дмитрий Игоревич Кудинов" with the VK account vk[.]ru/id6571635. Also, koley stated that Dragon Force Ransomware Group has contacts in the FSB, such as RansomHub. koley stated that the attack on RansomHub was a declaration of war between the two cybercriminal groups.

Dragon Force: Possible Attacks on Everest, LockBit, BlackLock (Mamona) Ransomware Groups

On March 18, 2025, Dragon Force Ransomware Group announced that it was operating as the Dragon Force ransomware cartel, and 24 hours later, it was observed conducting DDoS attacks and defacements against competitors' extortion websites, such as BlackLock Blog and Mamona Blog. Both websites are variants of El Dorado Ransomware Group and are operated by the same threat actor, "$$".

Later, on April 5, 2025, the extortion website named "Everest Ransom Team" used by the ransomware group Everest went offline after being apparently hacked and defaced over the prior weekend. Victim listings on the website were replaced by the message "Don't do crime CRIME IS BAD xoxo from Prague." It is not clear whether the incident is legitimate or who may be behind it (the same message was posted by an unknown user to LockBit's administrator affiliate panel — available in LockBit Leaked Chats), as law enforcement disruption operations, which have expanded in recent years, usually replace the websites they target with a splash page announcing the operation and identifying the agencies involved. The Everest blog defacement does not purport to come from a law enforcement agency, and no affiliates have been identified complaining about being "exit-scammed" on dark web forums. As of this writing, the extortion blog continues operating. However, it is possible that LockBit and Everest ransomware groups were targeted by Dragon Force.

Impact on Payments, Target Strategies, and Profitability

Since the beginning of Operation Endgame and multiple other successful law enforcement operations worldwide, Insikt Group has analyzed reports and statistics related to the financial gains and losses of ransomware operators and identified that they have been receiving fewer ransom payments since 2024, and this trend is continuing in the first half of 2025. In addition, exploitation of vulnerabilities, phishing attacks, and attacks via malicious emails are primary attack vectors to infect victims with ransomware.

Analysis of the reporting related to ransom payments indicates that the average ransomware payments in the first half of 2025 slightly decreased:

- Sophos released the report "The State of Ransomware" on June 30, 2025, which indicates that 32% of ransomware attacks resulted from vulnerability exploitation; data decryption rates decreased to 50% in 2025 (70% in 2024). Average (median) ransom demands decreased by 34% to $1,324,439, down from $2 million in 2024. Average (median) ransom payments dropped by 50% in 2025 ($1 million) from 2024 ($2 million).
- Coveware released a report on May 1, 2025, that indicates that an average ransom payment in Q1 2025 was $552,777 (-0.2% in comparison with Q4 2024). The median ransom payment in Q1 2025 was $200,000 (+80% in comparison with Q4 2024).
- Chainalysis reported on February 5, 2025, that in 2024, ransomware operators earned approximately $813.55 million in ransom payments, which indicates a 35% decrease from 2023, with $1.25 billion in ransom payments. Also, data leak websites posted more victims in 2024 than in any year prior; however, these data extortion websites often list already public information or repost from other sources to mislead and scam victims, law enforcement, and cybersecurity researchers. Another significant reason for that was likely the collapse of two major ransomware groups in 2024: LockBit 3.0 ("Operation Cronos," February 2024) and ALPHV (which performed an exit scam in January 2024).

Emerging ransomware groups cannot achieve the same scale of operations and market share as the above-mentioned variants.

Outlook

The Russian cybercriminal ecosystem is unlikely to contract — it will continue to reconfigure. We assess with high confidence that selective Russian enforcement will keep burning expendable monetization and infrastructure nodes while insulating high-utility operator circles, sustaining a conditional safe haven that adapts, rather than yields, to Western pressure. Over the next six to twelve months, Russian authorities will likely prioritize actions against low-utility enablers (such as cash-out brokers and politically sensitive hosting services tied to domestic optics) while avoiding decisive action against operators perceived to have intelligence or geopolitical value. Expect more Cryptex/UAPS-style cases and continued ambiguity around elite figures named in Western actions.

Cash-out friction will rise as seizures, sanctions, and episodic Russian cases disrupt trusted rails, prompting diversification through mixers, OTC brokers, and friendly jurisdictions. The result is higher transaction costs and delays, not a collapse of revenue. In parallel, trust erosion on forums will continue to push recruitment and negotiations from open marketplaces into semi-closed circles that require deposits, KYC-lite checks, and cultural gating. Open RaaS advertisements will persist at the margins to feed volume, while credible brands harden gates to protect continuity.

Business model churn will persist. We expect continued growth of data-extortion-only offerings, triple-extortion add-ons such as DDoS and call pressure, and investment-style affiliate schemes. Temporary privatization — going quiet under pressure, then resurfacing when attention shifts — will remain a common resilience pattern, as seen in commodity infostealer ecosystems. The net effect: shorter public exposure cycles and longer private monetization windows.

OPSEC will get heavier but remain uneven. Threat actors will keep migrating off centralized platforms and stacking toolchains (Tails, virtual machines [VMs], and hidden volumes), yet usability gaps and misconfigurations will continue to create seams defenders can exploit — especially during affiliate onboarding, payment pivots, and communications transitions. At the same time, builder leaks and rapid rebrands will keep spawning numerous low-credibility variants and new blogs, driving overall volume up while reducing signal quality; a smaller core of protected threat actors will retain disproportionate impact amid the noise.

Geography and target selection will remain politically bounded. Explicit carve-outs for CIS and BRICS and opportunistic swings tied to regional crises will endure, reflecting risk management inside the covenant. Threat actors will pursue high-yield opportunities while avoiding blowback in jurisdictions that endanger domestic cover. Western policy pressure will become more continuous as payment disclosures and bans expand, offensive authorities normalize, and multinational takedowns accelerate. Deterrence for elite operators will remain limited so long as swaps, lenient domestic outcomes, and political protection dilute perceived personal risk.

For defenders and policymakers, the implication is clear: durable impact comes from pressure on the incentives of protection as much as on the criminals themselves. Prioritize choke points in cash-out and infrastructure; instrument continuous measurement to detect oscillation between public and private operations; focus on seams in affiliate onboarding and negotiation cycles; and align sanctions and law-enforcement actions with diplomatic levers that raise the domestic cost of protection. In a managed market, the covenant adjusts to shocks; only by reshaping the calculus that sustains protection can disruption scale and persist.

Appendix A: Timeline of Russian Law Enforcement Events Related to Cybercrime

Possible Date of Operation	Operational Activity- or Law Enforcement-Related Event	Directly Associated with Operation Endgame
July 15, 2024	Russian authorities arrest Trickbot actor “Azot” (aka “Angelo”)	Yes
September 16, 2024	Russian authorities detain “Bio” from the Conti Group for an unknown period of time	No
October 2, 2024	Russian authorities conduct raids and arrest 100 people associated with Cryptex and UAPS	Yes
November 2024	Arrest of “Wazawaka”	No
January 2025	The Russian government seizes $10 million in Bitcoin (BTC) from a former Investigative Committee (SKR) member as part of a bribery case tied to leaders of the Infraud Forum	No
March 2025	Arrest of members associated with the Mamont banking trojan	No
April 4, 2025	The CEO of Aeza Group is arrested	No
June 2025	Four REvil threat actors are found guilty and sentenced to time served for trafficking in payment card data; Russian authorities also seize some money and property	No

(Source: Recorded Future)

Appendix B: List of New Ransomware TTPs Adopted after Operation Endgame

Changes TTPs	Ransomware Group
Data Extortion Model	Hunters International: Hunters International was one of the first RaaS groups to publicly announce its switch to a data extortion model. On August 14, 2024, on its extortion website, Hunters International stated that the number of ransom payments significantly decreased, and the primary reason for that was not a specific affiliate member program or quality of ransomware. The primary reason for that was publicity. According to the threat actors, the only possible variant is to receive ransom to target critical infrastructure; however, if the authorities do not authorize the ransom payment, there is no chance of earning money. Hunters International Group decided to exfiltrate data and not deploy

Changes TTPs	Ransomware Group
	ransomware. After that announcement, Hunters International stopped displaying ransom notes and renaming encrypted files. Anubis RaaS: Anubis Ransomware Group used a different tactic to entice affiliates. In late February 2025, the threat group debuted an affiliate model that features two modes. On February 23, 2025, the threat actor “superSonic” advertised the Anubis RaaS affiliate program on the forum Ramp and introduced two models: ransomware and data exfiltration. The data exfiltration business model allows users to send exfiltrated data from companies to Anubis, who would then conduct the extortion process via their extortion blog. In addition to Hunters International and Anubis, BianLian Ransomware Group was also observed switching from ransomware to data extortion operations.
Call Lawyer Option	Ransomware groups continued to strengthen their triple extortion techniques in addition to DDoS attacks and phone call services against already compromised victims. For example, on May 4, 2025, the threat actor Haise, a member of Ramp Forum and a member of Qilin Ransomware Group, announced that Qilin RaaS affiliate program was offering to its members an automated “call lawyer” service. According to the threat actor, the service includes the following options and benefits: • A legal “assessment” of compromised data • A legal classification of the violations depending on specific jurisdictions • A legal assessment of potential lawsuits, their costs, and reputation damages • Ability to conduct negotiations for the victims directly with a lawyer • A legal consultation regarding performing maximum damage to victims if they refuse to cooperate In addition, on May 5, 2025, the ransomware group implemented additional features, such as a file-sharing storage with up to 1 TB of data capacity, a spamming tool, its own pool of “journalists” who, in cooperation with lawyers, can help to create texts for publication on the extortion blog as well as to help with ransomware negotiations.
Investment Affiliate Program	On June 21, 2025, the threat actor “Nova”, on the forum Ramp, was hiring affiliate members for the new “Nova Access Investment Affiliate Program.” According to the threat actor, this investment affiliate program will be used for investment in the compromised network targeted by affiliate members. “The market value will be determined by the victim's ransom amount, depending on the region, target type, and those who provide larger victims will yield a more successful investment,” stated the threat actor. The Nova RaaS team was going to onboard investors via Session Messenger, where they could receive a trust badge. The description of the program also indicated that “this badge will grant you access to Nova's private chat server for enhanced privacy and a higher percentage of the ransom value, make sure that we will give you full access to Chat negotiation, and you will be able to see chat with victims.” On July 29, 2025, the ransomware operators stopped the Nova Investment Affiliate Program. They stated that instead, they would introduce another program that would be helpful for other members who cannot make deposits. The new program should allow new members to use Nova Ransomware Group’s resources and services for free if they provide one high-revenue access based in the US or the EU.

Changes TTPs	Ransomware Group
Hacker-for-Hire Model	In July 2025, Insikt Group observed the activities of D4rk 4rmy Blog, a dark web “name-and-shame” extortion blog likely operated by D4rk 4rmy (also known as “D4rk4rmy”) Ransomware Group. The extortion website contains the Chinese phrase “共产主义勒索软件党,” which is translated into English as “Communist Ransomware Party.” The threat group offers a hacker-for-hire service. It stated that it is an established group and is looking for experienced partners to cooperate. It only accepts Chinese, Russian, and English-speaking threat actors “who must be fluent in these languages” (likely in one of these three languages).
Dragon Force: Cartel and Premium RaaS	On April 24, 2025, “dragonforce”, a member of Ramp Forum and representative of Dragon Force Ransomware Group, stated that they would release RansomBay, a project that will target “Tier 1” countries with revenue up to $150 million. In addition, on September 15, 2025, Dragon Force Ransomware Group announced a coalition with Qilin and LockBit (LockBit 5.0 RaaS released on September 3, 2025, with an updated functionality). As of writing, Insikt Group cannot evaluate whether the threat groups completely combined teams, efforts, and resources or whether the statement was made to intimidate or mislead other rivalries of Dragon Force.

(Source: Recorded Future Data)

Appendix C: List of Targeted Entities Under Operation Endgame

Season Number	Threat Actor/Variant	Relevant Actions
Season 1	IcedID	Seizures and takedown
Season 1	SystemBC (“Psevdo”)	Seizures
Season 1	Pikabot	Arrests
Season 1 and Season 2	Smokeloader (“Greenhorse”)	Seizure Identification of customers
Season 1	BumbeleBee Loader	Seizures
Season 1 and Season 2	Trickbot	Video released
Season 1	Latrodectus	Seizure Video release
Season 2	Qakbot	Indictment Seizure
Season 2	DanaBot	Indictment Seizure
Season 1 and Season 2	Emotet (“Odd”)	Video release Seizure
Season 1	Cryptex	Video release
Season 1	Gold	Russian arrests and seizures Video release

Season Number	Threat Actor/Variant	Relevant Actions
Season 2	AVCheck	Seizure
Season 1 and Season 2	Conti Ransomware Group	EU Most Wanted list

(Source: operation-endgame[.]com)