ZEROFOX INTELLIGENCE

Brief

The Evolution of the Cybercrime-as-a-Service Market

B-2026-07-27a

Classification: TLP:CLEAR

Criticality: Low

Intelligence Requirements: Phishing, Ransomware, Threat Actor

July 27, 2026

Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were identified prior to 10:00 AM (EDT) on July 27, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Brief | The Evolution of the Cybercrime-as-a-Service Market

| Key Findings

- Over the past decade, cybercrime has almost certainly reorganized from largely self-contained intrusions into a specialized service economy in which discrete capabilities are bought and sold as products.
- Ransomware-as-a-service (RaaS) very likely became the commercial center of this ecosystem, professionalizing through successive brands into affiliate operations with profit-sharing, recruitment, technical support, and brand management.
- Extortion tradecraft escalated from simple encryption to “double extortion”: pairing encryption with the threat to publish stolen data. This was popularized around late 2019 and subsequently adopted across the RaaS landscape, often with dedicated data-leak sites and additional pressure tactics.
- The service model extended far beyond ransomware into phishing-as-a-service, initial access brokering, infostealer subscriptions, malware delivery, and distributed denial of service (DDoS)-for-hire, all supported by dark web markets, bulletproof hosting, and cryptocurrency laundering infrastructure.

- A sustained, multinational law-enforcement campaign repeatedly disrupted the ecosystem—yet resilience and rebranding were the recurring response, with several operations re-emerging within days to months.
- Generative artificial intelligence (GenAI) is an emerging accelerant rather than a demonstrated transformation. Criminal AI tooling appeared in mid-2023, and threat actors are very likely adopting AI faster than defenders can adapt to it. However, ZeroFox assesses the publicly available, corroborated evidence does not yet support specific claims about the scale of AI-driven growth.

The Service Model Takes Shape

From 2015–2026, ZeroFox has observed an increasing trend towards cybercrime specialization. Rather than a single actor owning the full attack chain, distinct providers sell access, tooling, delivery, and extortion as separate products. This service model serves as a complex web of interdependence, with initial access brokers (IABs), dropper and loader services, and phishing kits as core pillars of the cybercrime-as-a-service (CaaS) market. This division of labor has almost certainly lowered the barrier to entry for less-skilled actors.

- The European Union Agency for Cybersecurity (ENISA) similarly identifies malware-as-a-service (MaaS) as a significant and rapidly evolving threat from mid-2023 onward.[1]

The economic logic is straightforward. Specialization very likely concentrates expertise, raises quality, and spreads risk: an access broker does not need to know how to negotiate a ransom, and a ransomware affiliate need not know how to breach a perimeter. The result is a market in which capability is rented rather than mastered, and the least-skilled participant can still mount a damaging attack by assembling purchased components. Over the past decade, what began as crude affiliate kits very likely matured into managed platforms with dashboards, customer support, tiered pricing, and—at the high end—reputation systems and dispute resolution that mirror legitimate software businesses.

[1] hXXps://www.enisa.europa[.]eu/topics/cyber-threats/threat-landscape

From Bespoke Crime to Commodity: The Roots

The commercialization of cybercrime goes back further than the last decade, and the precursors established the template. CryptoLocker, which emerged in late 2013 and spread through the GameOver Zeus botnet, demonstrated that file-encrypting ransomware paired with cryptocurrency payment could be enormously profitable. The U.S. Department of Justice has stated that CryptoLocker infected more than 234,000 computers by April 2014 and that victims paid more than USD 27 million in ransom in just the first two months of the campaign.[2] In June 2014, "Operation Tovar", a multinational action led by U.S. authorities with European partners, disrupted both the GameOver Zeus botnet—estimated at between 500,000 and one million infected nodes—and the underlying CryptoLocker infrastructure.[3]

In its earliest "as-a-service" forms around 2015–2016, the model was comparatively crude: affiliate kits let a buyer generate a ransomware sample in exchange for a share of the proceeds.[4] Detailed figures from this early period derive largely from contemporaneous industry reporting, rather than primary records, and are likely incomplete. However, the trajectory is well documented: the kit became a platform, and the lone operator gave way to affiliate networks.

Ransomware-as-a-Service Professionalizes

Beginning around 2016, RaaS almost certainly became the clearest example of cybercrime's industrialization. In the affiliate model, a core team develops and maintains the ransomware, operates the leak site and negotiation infrastructure, and recruits affiliates who carry out intrusions; proceeds are split, with affiliates typically taking the larger share.

- GandCrab, active from January 2018, exemplified this approach. It was advertised on Russian-language underground forums, reportedly enrolled 292 affiliates, and

[2] hXXps://www.justice[.]gov/archives/opa/pr/us-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware
[3] hXXps://www.fbi[.]gov/news/stories/gameover-zeus-botnet-disrupted
[4] hXXps://krebsonsecurity[.]com/2014/06/operation-tovar-targets-gameover-zeus-botnet-cryptolocker-scourge/

operated on a 60/40 split between affiliates and the developers.[5] When its operators announced "retirement" on May 31, 2019, they claimed to have earned more than USD 2 billion, averaging USD 2.5 million per week.[6] [Analyst Note: These figures were self-reported and have not been independently verified.]

- The subsequent REvil (aka Sodinokibi) operation was very likely a successor to GandCrab, based on overlaps in both code and the underground personas behind it.[7] REvil became one of the most damaging RaaS brands before its July 2021 supply chain attack on Kaseya prompted U.S. charges against an affiliate; in early 2022, Russia's Federal Security Service conducted raids against group members.[8][9] The lineage from GandCrab to REvil likely illustrates a defining feature of the ecosystem: brands are likely disposable, but the operators, tooling, and business model behind them almost certainly persist.

Case Study: DarkSide and the Colonial Pipeline

The May 2021 ransomware attack on Colonial Pipeline was almost certainly the most publicized attack of the era. The operator, DarkSide, was itself an RaaS brand whose affiliates reportedly retained roughly 70 to 80 percent of proceeds while the developers took the remainder.[10] The attack forced Colonial to shut down a pipeline that supplies a large share of the U.S. East Coast's fuel; it restarted approximately five days later, after fuel shortages and emergency declarations across multiple states.[11] Colonial reportedly paid a ransom of approximately 75 Bitcoin (BTC)—approximately USD 4.4 million at the time—and the Federal Bureau of Investigation (FBI), in a milestone for the use of

[5] hXXps://www.bleepingcomputer[.]com/news/security/gandcrab-raas-was-a-training-ground-for-malware-distributors/
[6] hXXps://www.bleepingcomputer[.]com/news/security/gandcrab-ransomware-shutting-down-after-claiming-to-earn-2-billion/
[7] hXXps://krebsonsecurity[.]com/2019/07/is-revil-the-new-gandcrab-ransomware/
[8] hXXps://www.justice[.]gov/opa/pr/ukrainian-arrested-and-charged-ransomware-attack-kaseya
[9] hXXps://cyberscoop[.]com/revil-fsb-arrests-russia/
[10] hXXps://krebsonsecurity[.]com/2021/05/a-closer-look-at-the-darkside-ransomware-gang/
[11] hXXps://www.cisa[.]gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years

blockchain tracing, recovered 63.7 BTC (roughly USD 2.3 million) the following month by obtaining the private key to the receiving wallet.[12][13][14][15]

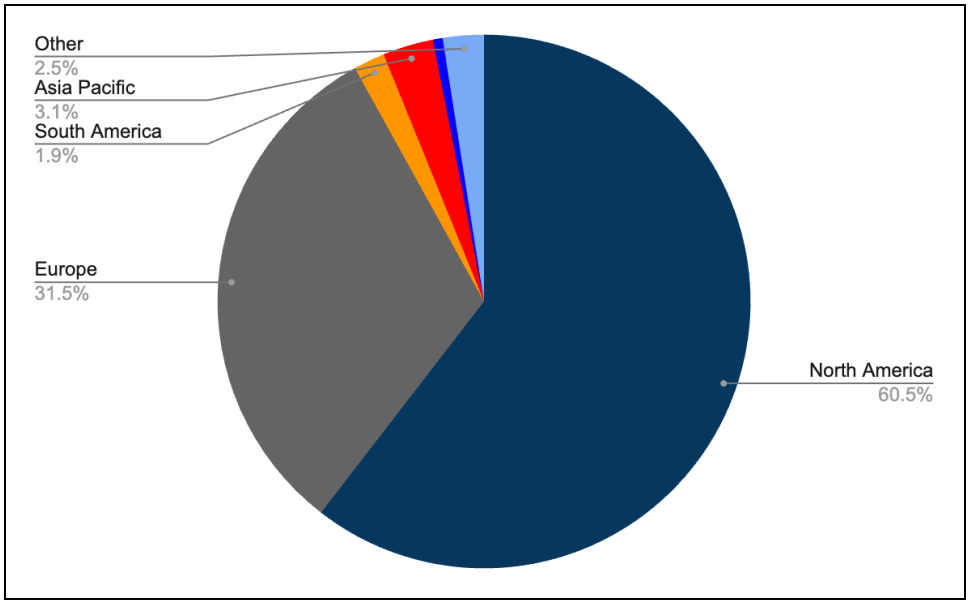
In a public statement, DarkSide sought to cast itself as apolitical, asserting that its goal was money rather than disruption, which was likely an attempt to manage reputational fallout and underscores how these operations weigh public perception.[16] DarkSide went dark within weeks before almost certainly re-emerging as BlackMatter, again demonstrating the rebrand reflex that has repeated throughout the last decade.

Conti and the Corporatization of Ransomware

If DarkSide showed the ecosystem's public face, the 2022 Conti leaks exposed its inner workings. After the group publicly backed Russia's invasion of Ukraine, an apparently internal cache of more than 60,000 messages was leaked that depicted a corporate-style organization of roughly 100 members with salaries, management hierarchy, human resources practices, and operational ties to the TrickBot and Emotet ecosystems. Blockchain analysis attributed at least USD 180 million in proceeds to Conti in 2021[17]—likely the most of any ransomware brand that year.

Beginning in April 2022, Conti attacked the government of Costa Rica, exfiltrating an estimated 672GB of data and prompting President Rodrigo Chaves to declare a national emergency on May 8, 2022, which is reportedly the first time a country declared such an emergency in response to a ransomware attack.[18] The high-profile exploit likely served as cover for Conti's own wind-down and rebrand.[19] The group dissolved around May 2022, and members likely dispersed into smaller successor operations such as Black Basta, Karakurt, and Royal.[20]

[12] hXXps://www.fbi[.]gov/news/press-releases/fbi-statement-on-compromise-of-colonial-pipeline-networks
[13] hXXps://www.justice[.]gov/archives/opa/pr
[14] hXXps://krebsonsecurity[.]com/2021/06/justice-dept-claws-back-2-3m-paid-by-colonial-pipeline-to-ransomware-gang/
[15] hXXps://www.bleepingcomputer[.]com/news/security/us-recovers-most-of-colonial-pipelines-44m-ransomware-payment/
[16] hXXps://krebsonsecurity[.]com/2021/05/a-closer-look-at-the-darkside-ransomware-gang/
[17] hXXps://www.cisecurity[.]org/insights/blog/the-conti-leaks-a-case-of-cybercrimes-commercialization
[18] hXXps://www.bleepingcomputer[.]com/news/security/costa-rica-declares-national-emergency-after-conti-ransomware-attacks/
[19] hXXps://krebsonsecurity[.]com/2022/05/costa-rica-may-be-pawn-in-conti-ransomware-groups-bid-to-rebrand-evade-sanctions/
[20] hXXps://www.bleepingcomputer[.]com/news/security/conti-ransomware-shuts-down-operation-rebrands-into-smaller-units/

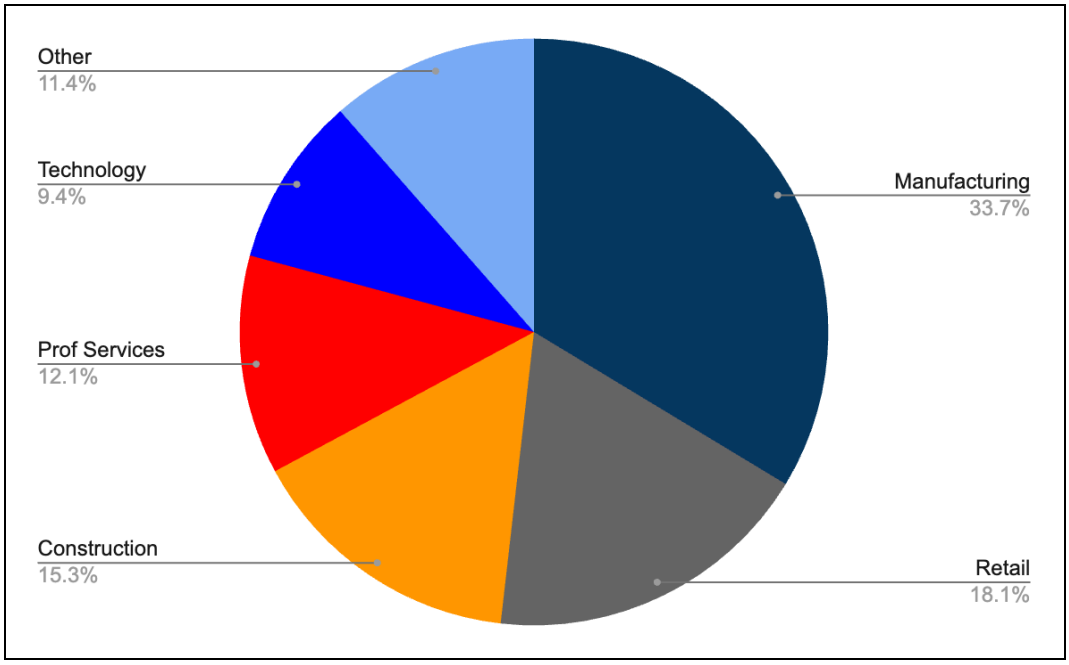


Conti attacks by region 2016–present
Source: ZeroFox Intelligence

LockBit and the Industrial Peak

LockBit likely represented the industrial peak of the RaaS model. Iterating through LockBit 2.0 in 2021 and LockBit 3.0 (also called LockBit Black) in June 2022, the operation professionalized aggressively—even launching what was billed as the first ransomware "bug bounty" program offering USD 1,000 to USD 1 million for vulnerabilities in its own tooling and infrastructure.[21] In a June 2023 advisory, U.S. and other Western authorities reported that LockBit had been the most-deployed ransomware variant globally in 2022 and was tied to roughly 1,700 attacks in the United States since 2020, extracting approximately USD 91 million from U.S. victims.[22]

[21] hXXps://www.bleepingcomputer[.]com/news/security/lockbit-30-introduces-the-first-ransomware-bug-bounty-program/
[22] hXXps://www.cisa[.]gov/news-events/cybersecurity-advisories/aa23-165a



LockBit attacks by sector 2016–present
Source: ZeroFox Intelligence

LockBit's scale became clearer after February 2024's Operation Cronos, in which a UK-led coalition seized 34 servers and recovered more than 1,000 decryption keys (reportedly part of a cache of thousands).[23][24] In May 2024, authorities unmasked and sanctioned the group's administrator, Russian national Dmitry Khoroshev ("LockBitSupp"), alleging that LockBit had attacked more than 2,500 victims across 120-plus countries (roughly 1,800 of them in the United States) and extracted at least USD 500 million in ransoms, of which Khoroshev had personally received more than USD 100 million.[25][26]

Extortion Escalates

As defenders improved backups and recovery, extortion tactics escalated to preserve leverage. The Maze operation likely popularized "double extortion" around late 2019: combining encryption with the theft of victim data and the threat to publish it on a public

[23] hXXps://www.nationalcrimeagency[.]gov[.]uk/news
[24] hXXps://www.bleepingcomputer[.]com/news/security/lockbit-ransomware-admin-identified-sanctioned-in-us-uk-australia/
[25] hXXps://www.justice[.]gov/archives/opa/pr/us-charges-russian-national-developing-and-operating-lockbit-ransomware
[26] hXXps://www.nationalcrimeagency[.]gov[.]uk/news/lockbit-leader-unmasked-and-sanctioned

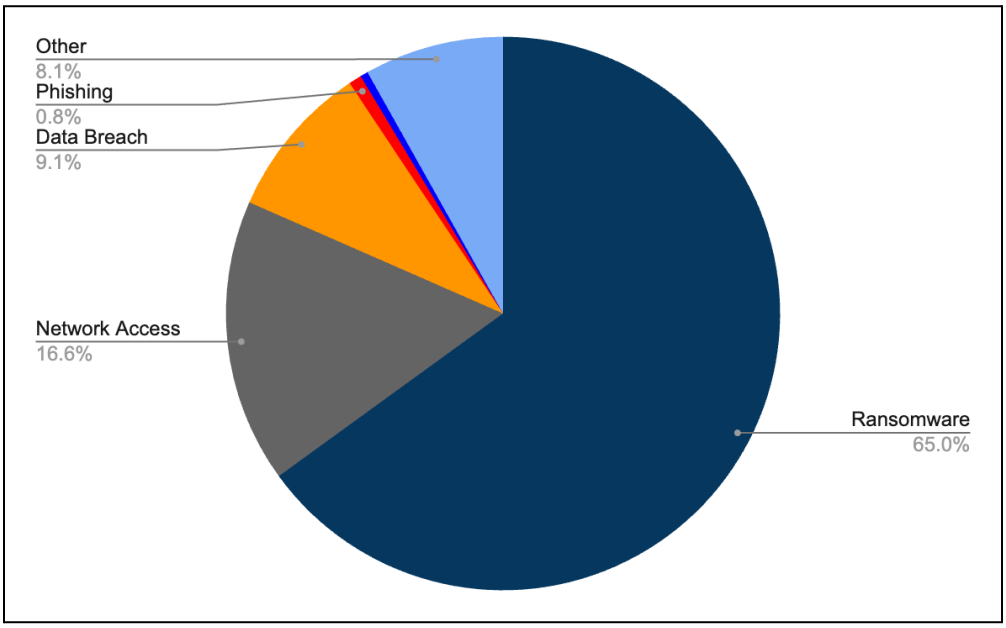
leak site. While some lower-profile data-theft-plus-encryption cases predate Maze, the practice it systematized became standard across the RaaS landscape. Government reporting on later brands, such as ALPHV/BlackCat, documents multi-faceted extortion as a defining feature of the model.[27]

Ransomware drew headlines, but the same service logic almost certainly reshaped the rest of the criminal supply chain. Phishing-as-a-service matured into turnkey platforms; the 16Shop platform (dismantled in an INTERPOL-coordinated operation in 2023) reportedly affected roughly 70,000 victims across 43 countries and generated more than 150,000 phishing domains.[28][29] Platforms such as LabHost harvested roughly 480,000 card numbers and more than one million passwords; it was disrupted in 2024 under Europol's Operation PhishOFF, leading to 37 arrests across 19 countries.[30][31] A notable technical advance in this category was the emergence of adversary-in-the-middle (AitM) kit platforms such as Tycoon 2FA and EvilProxy. These proxied a victim's live session to defeat multi-factor authentication (MFA) rather than merely harvesting static credentials, offering subscriptions reportedly in the range of roughly USD 100 to USD 1,000 per month.[32][33]

Credential theft was likewise commoditized through infostealer MaaS. The FBI reportedly tied Raccoon Stealer (leased for about USD 200 per month) to more than 50 million stolen credentials, and its alleged operator pleaded guilty in a U.S. district court.[34][35] The RedLine and META stealers were disrupted in 2024's Operation Magnus,[36][37] and in May 2025 authorities disrupted the LummaC2 stealer, which the FBI associated with roughly 1.7 million infection instances.[38] Upstream, malware delivery and botnet services such as

[27] hXXps://www.cisa[.]gov/news-events/cybersecurity-advisories/aa23-353a
[28] hXXps://www.interpol[.]int/en/News-and-Events/News/2023
[29] hXXps://www.bleepingcomputer[.]com/news/security/interpol-takes-down-16shop-phishing-as-a-service-platform/
[30] hXXps://www.europol.europa[.]eu/media-press/newsroom/news
[31] hXXps://www.bleepingcomputer[.]com/news/security/labhost-phishing-service-with-40-000-domains-disrupted-37-arrested/
[32] hXXps://www.proofpoint[.]com/us/blog/email-and-cloud-threats/tycoon-2fa-phishing-kit-mfa-bypass
[33] hXXps://blog.talosintelligence[.]com/state-of-the-art-phishing-mfa-bypass/
[34] hXXps://www.justice[.]gov/usao-wdtx/pr
[35] hXXps://thehackernews[.]com/2022/10/us-charges-ukrainian-hacker-over-role.html
[36] hXXps://www.justice[.]gov/usao-wdtx/pr
[37] hXXps://thehackernews[.]com/2024/10/dutch-police-disrupt-major-info.html
[38] hXXps://www.justice[.]gov/opa/pr

Emotet rented access to other crews; Emotet's 2021 takedown affected an estimated 1.6 million devices, and data retrieved in the takedown explicitly described Emotet's role in delivering payloads for other actors.[39]



All cyberattacks by type (2016–present)
Source: ZeroFox Intelligence

Two further trends framed the past decade. Denial-of-service was packaged as "booter" and "stressor" services that anyone could buy to launch attacks, prompting the multi-year Operation PowerOFF, which by May 2025 had seized more than 75 domains and charged at least 11 U.S. defendants.[40] At the same time, the exploit-kit model that had dominated the mid-2010s collapsed; contemporaneous reporting documented an approximately 93 percent drop in exploit-kit activity between January and September 2016, after which the criminal market shifted decisively toward phishing and purchased access.[41]

[39] hXXps://www.europol.europa[.]eu/media-press/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action
[40] hXXps://www.justice[.]gov/usao-cdca/pr
[41] hXXps://www.darkreading[.]com/cyberattacks-data-breaches/exploit-kit-based-attacks-decline-dramatically

- Booters and stressors are subscription-based services that allow anyone to launch denial-of-service attacks. While they are marketed as "stress-testing" tools, they are illegal and almost exclusively used for cybercrime.

The Enabling Infrastructure: Markets, Hosting, and Money

Underpinning these services were marketplaces, hosting, and payment rails. Dark web markets cycled through growth and takedown: AlphaBay and Hansa were seized simultaneously in 2017's Operation Bayonet;[42] the Hydra marketplace (which received roughly USD 5.2 billion in cryptocurrency since 2015 and accounted for an estimated 80 percent of dark net-market crypto volume in 2021) was dismantled in 2022;[43] and Genesis Market, advertising credentials and browser fingerprints from roughly 460,000 compromised devices, was taken down in Operation Cookie Monster in 2023.[44] "Bulletproof" hosting provided strategic infrastructure with near impunity, but international law enforcement soon caught up; the LolekHosted operator was charged in 2023 with facilitating roughly 400 ransomware attacks tied to about USD 146 million in ransoms.[45][46]

Over the last decade, cryptocurrency has been both the medium of payment and a growing avenue for enforcement. Laundering infrastructure became a distinct enforcement target: the U.S. Treasury sanctioned the mixer Tornado Cash in August 2022, citing more than USD 7 billion laundered since 2019—including over USD 455 million tied to North Korea's Lazarus Group.[47]

- Cryptocurrency mixer services obscure the origin of various crypto coins by pooling funds from many different users together and then distributing those same coins back out to new addresses controlled by those users.

[42] hXXps://www.europol.europa[.]eu/media-press/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation
[43] hXXps://www.justice[.]gov/archives/opa/pr
[44] *Ibid.*
[45] *Ibid.*
[46] hXXps://thehackernews[.]com/2023/08/lolek-bulletproof-hosting-servers.html
[47] hXXps://home.treasury[.]gov/news/press-releases/jy0916

In March 2023, the ChipMixer service was dismantled after processing more than USD 3 billion in illicit transactions, with roughly USD 17 million linked to some 37 ransomware strains.[48] Finally, the operator of the long-running Bitcoin Fog mixer was convicted in March 2024 of laundering approximately 1.2 million BTC over roughly 10 years.[49]

The Economics in Numbers

The scale of cybercrime throughout the last decade is visible in two complementary datasets. The FBI's Internet Crime Complaint Center (IC3), which captures voluntarily reported losses from U.S. complainants, recorded total internet-crime losses rising from roughly USD 4.2 billion in 2020 to about USD 10.3 billion in 2022, USD 12.5 billion in 2023, and USD 16.6 billion in 2024.[505152] Blockchain analytics, which track ransom flows on-chain, show ransomware payments specifically exceeding USD 1 billion in 2023 before falling roughly 35 percent to about USD 814 million in 2024. Providers attribute the decline in part to law enforcement action and greater victim resistance, with LockBit's second-half 2024 payments reportedly down about 79 percent after Operation Cronos.[5354]

- These figures measure different things and should not be conflated. IC3's ransomware-specific number for 2023 (about USD 59.6 million in reported losses) is far smaller than the on-chain total, very likely because most victims do not report—and reported losses exclude downtime and remediation.[55]
- Read together, the datasets describe a large and, by 2024, possibly plateauing criminal economy whose true size almost certainly exceeds any single tally.

The Disruption Campaign and Its Limits

The second half of the last decade has seen coordinated, international disruption campaigns. The FBI infiltrated the Hive ransomware operation, announcing in January 2023 that it had distributed decryption keys and prevented an estimated USD 130 million

[48] hXXps://www.justice[.]gov/archives/opa/pr
[49] hXXps://www.justice[.]gov/opa/pr/bitcoin-fog-operator-convicted-money-laundering-conspiracy
[50] hXXps://www.ic3[.]gov/Media/PDF/AnnualReport/2022_IC3Report[.]pdf
[51] hXXps://www.ic3[.]gov/AnnualReport/Reports/2023_IC3Report[.]pdf
[52] hXXps://www.ic3[.]gov/AnnualReport/Reports/2024_IC3Report[.]pdf
[53] hXXps://www.chainalysis[.]com/blog/ransomware-2024/
[54] hXXps://www.chainalysis[.]com/blog/crypto-crime-ransomware-victim-extortion-2025/
[55] hXXps://www.ic3[.]gov/AnnualReport/Reports/2023_IC3Report[.]pdf

in ransom payments across more than 1,500 victims in over 80 countries.[56] In December 2023, U.S. authorities disrupted ALPHV/BlackCat and distributed a decryption tool, foiling an estimated USD 68 million in demands,[5758] and in February 2024 the UK-led Operation Cronos struck LockBit. Marketplace and infrastructure takedowns (Emotet, Hydra, Genesis Market, Qakbot, and the mixer actions described above) widened the campaign well beyond ransomware brands.[59606162]

Operation Cronos message on LockBit site

Source: ZeroFox Intelligence

These actions imposed real costs, and tracked ransom payments fell in 2024.[63] Yet resilience was the recurring theme: ALPHV/BlackCat re-emerged on new infrastructure within days of its disruption, Qakbot operators reportedly remained active, and LockBit attempted to rebuild even after Cronos. The pattern of disposable brands and persistent

[56] hXXps://www.justice[.]gov/archives/opa/pr/us-department-justice-disrupts-hive-ransomware-variant
[57] hXXps://www.justice[.]gov/archives/opa/pr
[58] hXXps://www.cisa[.]gov/news-events/cybersecurity-advisories/aa23-353a
[59] hXXps://www.europol.europa[.]eu/media-press/newsroom/news
[60] hXXps://www.justice[.]gov/archives/opa/pr
[61] *Ibid.*
[62] hXXps://www.fbi[.]gov/news/stories
[63] hXXps://www.chainalysis[.]com/blog/crypto-crime-ransomware-victim-extortion-2025/

operators—visible from GandCrab to REvil and from Conti to its splinters—indicates that disruption tends to degrade specific operations and erode criminal trust rather than dismantle the underlying market. These disruption campaigns very likely raised friction across the ecosystem but most certainly did not end it.

Analyst Commentary

The defining development of the 2015–2025 decade was almost certainly structural: the commoditization of offensive capability into a specialized service economy. Law enforcement disruption, while increasingly effective at imposing costs, is unlikely to durably dismantle the ecosystem on its own. The repeated pattern of re-emergence and rebranding—together with the low barrier to spinning up replacement infrastructure—suggests that disruption raises friction and degrades specific brands rather than eliminating the market. The 2024 decline in tracked ransom payments is encouraging but should be read cautiously; providers note their figures are conservative and revised upward over time, and a single year is not a trend.

Geography is likely a persistent enabler. Much of the ecosystem operates from jurisdictions that do not extradite to Western countries, and many RaaS builds are configured to avoid encrypting systems that use Commonwealth of Independent States (CIS) or Russian-language locations—an observed pattern consistent with operators seeking to avoid law enforcement attention in their home territories.[64] This safe-haven dynamic very likely limits the durable impact of arrests and indictments, since named administrators such as LockBit's frequently remain beyond reach.

GenAI is the newest input into this model. Criminal AI tooling marketed under names such as WormGPT and FraudGPT appeared in mid-2023, and security researchers have documented criminal use of GenAI for phishing and business email compromise content.[65] Further, European law enforcement frames the current situation as a "velocity gap"— meaning adversaries adopt AI faster than defenders and investigators can adapt to it.[66] It is almost certain AI adoption across the cybercriminal service economy will continue to accelerate over the next 12 to 24 months.

[64] hXXps://krebsonsecurity[.]com/2021/05/try-this-one-weird-trick-russian-hackers-hate/
[65] hXXps://blog.talosintelligence[.]com/year-in-review-ai-based-threats/
[66] hXXps://www.europol.europa[.]eu/publication-events/main-reports/iocta-2026-evolving-threat-landscape

It is very likely the service-economy structure will persist and that specialization will deepen, with IABs and credential markets continuing to feed ransomware and fraud operations. It is also likely that extortion will remain data-centric, that MFA-bypass phishing will continue to spread, and that disrupted brands will continue to rebrand rather than exit. The strategic implication is that the threat is systemic rather than tied to any single group; defenders gain the most by targeting the shared building blocks—credential theft, phishing, and initial access—common to the entire market.

Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	**Sources may use** TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	**Sources may use** TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	**Recipients may NOT share** TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	**Recipients may ONLY share** TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. **Note that** TLP:AMBER+STRICT restricts sharing to the organization only.

	Green	Clear
WHEN SHOULD IT BE USED?	**Sources may use** TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	**Sources may use** TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	**Recipients may share** TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	**Recipients may share** TLP:CLEAR information without restriction, subject to copyright controls.

Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%