Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

From Oligopoly to Fragmentation: Market Structure and Law-Enforcement Disruption in the Ransomware-as-a-Service Economy

Niccolò Rinaldi

niccolo.rinaldi@unifi.it

University of Florence

Giulio Bello

University of Pisa

Chiara Tani

University of Florence

Research Article

Keywords:

Posted Date: November 11th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-11524943/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: No competing interests reported.

From Oligopoly to Fragmentation: Market Structure and Law-Enforcement Disruption in the Ransomware-as-a-Service Economy

Abstract

Cybercrime-as-a-Service (CaaS) is widely described as an industrialised market, yet the structure of that market is rarely measured. We study Ransomware-as-a-Service (RaaS) as an industry, using 29,162 victim claims published by 287 groups on data leak sites between January 2022 and September 2026. We combine a model of the CaaS supply chain, a mapping of ransomware and phishing services onto MITRE ATT&CK, and measures from industrial organisation and survival analysis. The market moved from a tight oligopoly to a fragmented one. The quarterly Herfindahl–Hirschman Index fell from 2,000–2,350 in early 2022, when LockBit alone posted up to 46% of claims, to 440–730 from 2024 onwards, about 28% less each year. The decline holds when known rebrands are merged into one organisation, when reposts, small groups or mass-exploitation campaigns are excluded, and in a second leak-site tracker. Brands are short-lived: the median brand stops posting after about nine months. After Operation Cronos in February 2024, LockBit's share fell from 20.7% to 1.0% within a year. Across seven law-enforcement operations against ransomware groups between 2023 and 2025, we find no detectable fall in market-wide claims, and the share lost by targeted groups was redistributed in the same way as in ordinary months. Disruption reshapes the market rather than shrinking it. We discuss implications for law enforcement, defenders and EU policy.

Keywords: Ransomware-as-a-Service, Cybercrime-as-a-Service, Market concentration, Law-enforcement disruption, Data leak sites, MITRE ATT&CK

1 Introduction

Cybercrime has become a division of labour. Malware developers, initial access brokers, affiliates and money launderers specialise in one stage of an attack and trade with each other, a pattern usually described as Cybercrime-as-a-Service (CaaS) (Huang et al. 2018). Ransomware-as-a-Service (RaaS) is its most visible product. A core team maintains the encryptor, the negotiation portal and the data leak site, and rents them to affiliates in exchange for a share of each ransom (Meland et al. 2020). Since 2019,

groups have added a second lever, double extortion: they steal data before encrypting it and publish victims who refuse to pay on leak sites hosted on Tor.

The language used to describe this ecosystem is economic. Reports speak of business models, affiliate programmes, market leaders and brand loyalty. Yet the structure of the market itself is rarely measured. Criminological work has asked whether cybercrime networks qualify as organised crime (Leukfeldt et al. 2017), and how much of the underground economy is actually commoditised (van Wegberg et al. 2018; Akyazi et al. 2021). Studies of ransomware groups have mostly relied on single cases, notably the leaked chats of Conti (Ruellan et al. 2024; Paternoster et al. 2025; Whelan et al. 2026), or on court files and interviews (Matthijsse et al. 2023). Leak-site data have been used to estimate how many attacks occur (Meurs et al. 2026) and to describe their concentration at one point in time (Müller and Yannikos 2026). What is missing is a longitudinal view: how concentrated the RaaS market is, how it changes, and how it responds when law enforcement removes its largest firm.

This question matters for policy. Between December 2023 and August 2024, law enforcement disrupted ALPHV/BlackCat, LockBit and Dispossessor (U.S. Department of Justice 2023b; National Crime Agency 2024; Help Net Security 2024). Ransom payments fell by an estimated 35% in 2024, while the number of victims posted on leak sites kept rising (Toulas 2025). If disruption only redistributes affiliates across new brands, the right measure of success is not the fall of one group but the shape of the market that follows. Research on other illicit online markets suggests that the effects of such operations are often short-lived (Décary-Hétu and Giommoni 2017; Collier et al. 2019).

We address four research questions:

- **RQ1.** How concentrated is the RaaS market, and how has concentration evolved since 2022?
- **RQ2.** How long do ransomware brands survive, and how fast is the market renewed by new entrants?
- **RQ3.** How did the market respond to the disruption of its dominant operator, LockBit, in February 2024, and to law-enforcement operations against ransomware groups more generally?
- **RQ4.** Do groups specialise by sector, and how exposed are the EU and Italy?

The paper makes three contributions. First, it brings together the qualitative model of the CaaS supply chain and a mapping of ransomware and phishing services onto MITRE ATT&CK (Strom et al. 2018), showing how the two services connect along one value chain. Second, it provides, to our knowledge, the first longitudinal measurement of RaaS market structure, using the Herfindahl–Hirschman Index (HHI), brand survival curves and an event study of seven law-enforcement operations. We show that a static snapshot of concentration, such as the one in Müller and Yannikos (2026), is reproduced in our data but hides a steep decline over time. Third, it shows that leak-site data need careful cleaning before they can support economic claims, because some groups republish other groups' victims, and it tests the results against brand lineages and a second tracker. The data pipeline and analysis code are released for replication.

Section 2 reviews related work. Section 3 describes the CaaS supply chain and Section 4 maps its two key services onto ATT&CK. Section 5 presents data and methods, Section 6 the results. Section 7 discusses implications, Section 8 limitations, and Section 9 concludes.

2 Related work

2.1 Cybercrime as a service economy

Huang et al. (2018) model cybercrime as a value chain of 24 value-added activities that can be offered "as a service". This framing implies specialisation, trade and cooperation between actors, and it underlies most current descriptions of CaaS. Empirical tests of the framing are more cautious. Measuring sales on online anonymous markets, van Wegberg et al. (2018) found that the commoditisation of attack tools was more limited than commonly assumed, with much of the trade concentrated in cash-out services. Akyazi et al. (2021) measured CaaS offerings over eleven years of a large cybercrime forum and found evidence for only 9 of 28 known CaaS types. Studying markets for remote access trojans, Kool et al. (2026) found that CaaS markets lower the barriers to entry through accessible tools, user-friendly design and trust signals between buyers and sellers. Musotto and Wall (2022) analysed a DDoS stresser service and found an e-commerce business model, a distributed rather than hierarchical organisation and a comparatively low income. Meland et al. (2020), after two years of netnographic observation of darknet markets and forums, found few RaaS offerings for sale, many of doubtful authenticity. They also proposed a value chain of the actors in this market, which we build on in Section 3. From 44 court files and ten expert interviews, Matthijsse et al. (2023) reconstructed the crime script of ransomware attacks. They describe a professionalised ecosystem in which groups outsource parts of the attack, offer victims a form of customer service and rely on facilitators such as cryptocurrency mixers and exchanges.

Criminologists have also asked how organised these actors are. Studying 40 networks involved in financial cybercrime, Leukfeldt et al. (2017) found that most had the minimal structure required by broad definitions of organised crime. Few showed the violence, corruption or control over distribution emphasised by stricter definitions. Comparing ten closed investigations of financially motivated cybercriminal networks, Lusthaus et al. (2024) found relatively stable business models and a common division between the attack and the money components. Whelan et al. (2024) revisited the question for ransomware. Using von Lampe's framework, they argue that some ransomware groups qualify as organised crime under a broader conception, and that the debate should move beyond whether organised cybercrime exists. Di Nicola et al. (2025) applied the constitutive elements of classical definitions to 71 judicial cases combining cybercrime with participation in an organised criminal group. The groups consistently showed collaboration, continuity, profit orientation and network organisation, but rarely violence, corruption or monopolistic ambitions. Our measurement speaks to one element of these definitions: whether any ransomware group controls its market.

2.2 Ransomware groups as organisations

The leak of Conti's internal chats in 2022 offered a rare view inside a RaaS operator. Ruellan et al. (2024) applied topic modelling to the chats and found that Conti operated like a firm that needed managers and business functions alongside technical staff. Paternoster et al. (2025) combined social network analysis and content analysis of 168,740 leaked messages and found a hierarchy with defined leadership roles and task specialisation. Whelan et al. (2026) analysed the group's organisational units, functions, roles and communication patterns, and Martin et al. (2025) showed that Conti used human-resources practices, such as those predicted by organisational support theory, to retain its workers. Beyond Conti, Phipps and Nurse (2026) reviewed more than 500 sources on Conti, LockBit and ALPHV/BlackCat. They found shared traits, including business-like operations, brand-building, strong leadership and the RaaS model, and recommended countermeasures such as undermining group branding, targeting affiliate networks and publicly exposing key members. Nershi (2025) combined 4,194 double-extortion victims posted on leak sites between May 2019 and April 2022 with over 60,000 leaked Conti messages to document informal alignment between Russia-based groups and the Russian state, including increased attack activity by Russia-based groups before Western elections. Less is known about affiliates. In a pay-per-install programme spreading Android banking trojans, Paquet-Clouston and García (2022) found labour-intensive and precarious work, with incomes below affiliates' expectations. These studies describe the firm. We describe the industry in which such firms compete, and in particular how often its brands are created and abandoned.

2.3 Leak sites as a data source

Leak sites are the only large, public and continuous trace of ransomware activity, and community aggregators such as ransomware.live, RansomLook and ransomwatch scrape them daily. Their limits are well known. They show only victims who did not pay, or not yet; claims can be false, delayed or reposted; and the aggregator assigns sector and country. Meurs et al. (2026) used leak-site data as one of three sources in a capture–recapture model of ransomware attacks against Dutch firms, and estimated that only about 40% of attacks on large and medium companies were reported to police. Müller and Yannikos (2026), the closest work to ours, merged ransomware.live and RansomLook into 27,629 posts from 325 groups. They report that the top 5% of groups account for about half of all posts and describe temporal, geographic and sectoral patterns. Their concentration measures are a single snapshot, however; they do not track concentration over time, model brand survival or study interventions. Payment data are a complementary source: Cable et al. (2024) identified more than $900 million in ransomware payments on the blockchain and used them to follow groups over time. Payments measure revenue rather than visible output, but they cover far fewer groups than leak sites.

2.4 Disrupting illicit online markets

Research on other illicit online markets offers expectations for RQ3. Décary-Hétu and Giommoni (2017) found that Operation Onymous, which took down several drug cryptomarkets in 2014, had effects that were limited in time and scope: the impact on cryptomarkets lasted less than two months, some participants displaced their activity to other markets, and prices did not rise. Collier et al. (2019) evaluated police interventions against booter services for denial-of-service attacks and found that individual takedowns produced significant but short-lived falls in attacks, while wider coordinated operations, such as the closure of the HackForums booter market and the FBI's December 2018 operation, reduced attacks for several weeks and changed the structure of the market. Industry analyses of Operation Cronos report a similar pattern. LockBit kept posting after the takedown, but many of its post-disruption victims were reuploads of attacks that predated it (Boyton 2024). When RansomHub went offline in April 2025, its affiliates reportedly moved to Qilin, while DragonForce claimed control of it (Lakshmanan 2025). No study, to our knowledge, has measured these shifts across the whole RaaS market or compared them across operations.

3 The CaaS supply chain

3.1 Actors and stages

A modern ransomware attack is rarely the work of one actor. Following the value-chain view of Huang et al. (2018) and Meland et al. (2020), we distinguish five specialised roles (Fig. 1).

Developers and RaaS operators build and maintain the technical core: encryptors, negotiation portals, leak sites and the affiliate panel. Phishing kits and information stealers are produced by similar specialists and sold to anyone who pays. Their tools are not necessarily used by their authors. They are packaged as products, with updates, documentation and support.

Initial access brokers (IABs) breach corporate perimeters and resell access. Typical entry points are stolen credentials harvested by infostealers, exposed remote desktop and VPN services, and unpatched edge devices. ATT&CK now records this purchase as a distinct technique, Acquire Access (T1650), and its procedure examples include ransomware groups buying credentials from IABs. Outsourcing intrusion lets affiliates log in with valid accounts instead of breaking in, which helps them blend into legitimate traffic.

Affiliates perform the hands-on-keyboard part of the attack: privilege escalation, lateral movement, data theft and, finally, encryption. They choose victims, adapt to defences in real time and run the negotiation.

Extortion and publication is where the attack becomes public. Victims who do not pay are listed on the group's leak site, with samples of stolen data and a countdown. This name-and-shame step is the trace analysed in this paper.

Money launderers convert ransoms paid in cryptocurrency into usable funds through mixers, cross-chain bridges and exchanges with weak controls. Law-enforcement crackdowns on mixers and on exchanges that ignore know-your-customer

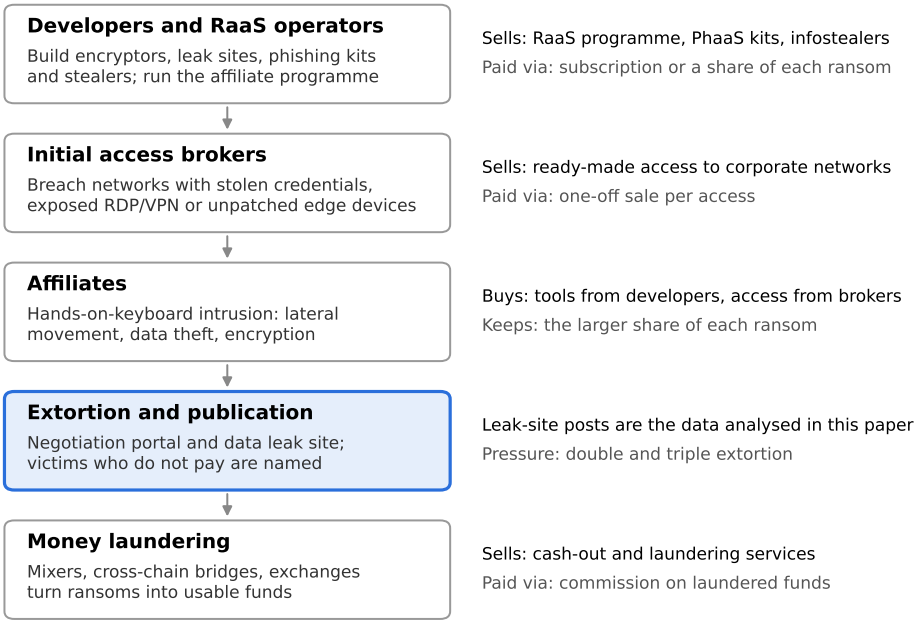


Fig. 1 The Cybercrime-as-a-Service supply chain behind a ransomware attack. The highlighted stage, leak-site publication, is the trace measured in this paper

rules have made laundering harder (Toulas 2025). Laundering is not always sophisticated: blockchain analysis of 182 addresses belonging to 56 members of Conti showed that most proceeds were concentrated in a single service, usually an exchange, and that mixers appeared in only 8% of transactions (Nazzari 2023).

3.2 Monetisation

Two revenue models coexist. Tools such as phishing kits and stealers are mostly sold by subscription or one-off purchase, like legitimate software-as-a-service. RaaS programmes instead use profit sharing: the affiliate pays nothing up front, keeps the larger share of each ransom and passes a percentage to the operator. Profit sharing lowers the affiliate's entry cost and gives the operator an incentive to keep improving the product.

The same infrastructure is also used by state-linked actors. Nershi (2025) documents informal but mutually beneficial ties between Russia-based ransomware groups and the Russian state. Microsoft reports that in 2025 a North Korean state actor took part in a RaaS programme as an affiliate for the first time, and expects RaaS and state actors to build affiliate networks able to survive takedowns (Microsoft 2025, pp 14, 48). State participation blurs the line between crime and espionage and complicates attribution.

3.3 What this structure implies for the market

The supply-chain view yields three expectations that we test in Section 6. First, because affiliates bring their own skills and access, they can move between programmes at low cost. Operators therefore compete for affiliates, and no single brand should be able to hold a dominant share for long (**E1**, declining concentration as the market matures). Second, a brand is cheap to create and easy to abandon, since the code, the affiliates and the access can be relocated. Brands should therefore be short-lived relative to the people behind them (**E2**, high turnover). Third, removing a brand removes neither its affiliates nor the demand for extortion. A takedown should therefore redistribute activity to rivals and new brands rather than reduce it (**E3**, displacement).

4 RaaS and PhaaS through MITRE ATT&CK

Two services carry most of the CaaS supply chain: Phishing-as-a-Service (PhaaS), which produces credentials and session tokens, and RaaS, which turns access into extortion. MITRE ATT&CK describes adversary behaviour as tactics (the goal of a step) and techniques (how the goal is reached) (Strom et al. 2018). Mapping both services onto the same matrix shows where they meet.

4.1 Ransomware-as-a-Service

A RaaS intrusion follows four phases. Initial access is usually bought from a broker or obtained with valid credentials, exposed remote services or a public-facing exploit. The affiliate then escalates privileges and moves laterally, often with legitimate remote monitoring and management (RMM) tools that are hard to tell apart from administrators' activity. Data are exfiltrated before encryption, which enables double extortion: the threat to publish stolen data on the leak site. Encryption comes last, preceded by the deletion of backups and shadow copies. Some groups add a third lever, such as DDoS or contacting the victim's customers. Others skip encryption and rely on data theft alone, because better backups have made encryption less decisive.

4.2 Phishing-as-a-Service

A phishing kit bundles cloned login pages, a backend that forwards captured credentials, evasion modules against scanners and filters, and operating instructions. Modern kits target multi-factor authentication (MFA). Adversary-in-the-middle (AiTM) kits proxy the real login page and capture the session token as well as the password. Device-code phishing tricks the user into authorising the attacker's device through a legitimate sign-in flow. ClickFix lures persuade users to paste a command into the Windows Run dialog, which loads the payload directly in memory. Email bombing floods a mailbox to hide security alerts, often as a prelude to a fake help-desk call.

4.3 Mapping

Table 1 maps these behaviours onto ATT&CK (Enterprise matrix, version 20, as listed in the online knowledge base in October 2026). The two services overlap in initial access, execution and persistence. PhaaS ends where RaaS begins: credentials and tokens obtained through phishing are one of the inputs that brokers resell and affiliates use.

Table 1 RaaS and PhaaS behaviours mapped to MITRE ATT&CK

Tactic	Technique (ID)	RaaS	PhaaS	Detection signal
Resource Development	Acquire Access (T1650)	✓		Corporate access offered on underground forums (external intelligence)
Resource Development	Acquire Infrastructure: Domains (T1583.001)		✓	Newly registered look-alike domains
Initial Access	Valid Accounts (T1078)	✓	✓	Sign-ins from unusual locations, impossible travel
Initial Access	External Remote Services (T1133)	✓		VPN/RDP sessions at unusual hours or from unusual networks
Initial Access	Exploit Public-Facing Application (T1190)	✓		Exploitation of edge devices and remote-management products
Initial Access	Phishing (T1566)	✓	✓	Links to new domains or abused trusted platforms
Execution	User Execution: Malicious Copy and Paste (T1204.004)	✓	✓	Shell launched from the Run dialog after clipboard activity (ClickFix)
Execution	Command and Scripting Interpreter: PowerShell (T1059.001)	✓	✓	Script hosts spawned by explorer.exe
Stealth	System Binary Proxy Execution: Mshta (T1218.005)	✓	✓	mshta.exe loading remote content
Credential Access	Adversary-in-the-Middle (T1557)		✓	Session token reused from a different IP address
Credential Access	Steal Application Access Token (T1528)		✓	Device-code sign-ins by users who never use that flow
Persistence	Account Manipulation: Device Registration (T1098.005)	✓	✓	New MFA method registered after an anomalous sign-in
Collection	Email Forwarding Rule (T1114.003)		✓	Forwarding rules to external domains
Defense Impairment	Disable or Modify Tools (T1685)	✓		Changes to antivirus or EDR exclusions
Lateral Movement	Remote Desktop Protocol (T1021.001)	✓		Internal RDP between hosts that do not normally connect
Command and Control	Remote Access Tools (T1219)	✓		Unapproved RMM tools on endpoints
Exfiltration	Exfiltration Over Web Service (T1567)	✓		Large uploads to cloud storage
Impact	Inhibit System Recovery (T1490)	✓		Deletion of shadow copies and backups
Impact	Data Encrypted for Impact (T1486)	✓		Mass renaming or encryption of files
Impact	Email Bombing (T1667)	✓	✓	Burst of subscription emails to one mailbox

The table also explains why market fragmentation, documented below, matters for defence. When many small brands share the same affiliates, tools and access sources, defenders gain more from detecting techniques than from tracking group names. Technique coverage changes slowly; brand names change every few months.

5 Data and methods

5.1 Data

We use the public API of ransomware.live (version 2), a community aggregator that monitors ransomware leak sites and records each victim post (ransomware.live 2026). We downloaded all posts discovered between January 2022 and September 2026, month by month, on 24 October 2026. The raw data contain 30,085 records. Each record includes the victim name and domain, the group, the discovery date, an estimated attack date, and the victim's country and sector as assigned by the aggregator.

The unit of analysis is a *claim*: one victim published by one group. Claims are not attacks. Victims who pay are usually never posted, posts can be false or delayed, and the aggregator's coverage of groups has grown over time. We return to these limits in Section 8. For market structure, the relevant point is that leak-site claims measure the *publicly visible output* of each brand, which is also what affiliates, victims and competitors observe.

To check that results do not depend on one aggregator, we compare them with ransomwatch, an open-source tracker that published its scraped leak-site posts until June 2025 (Highet 2025). We use its posts from January 2022 to December 2024, when its coverage was still complete, and apply the same normalisation and deduplication. The two sources are not fully independent, because ransomware.live was initially built on ransomwatch's work (Poireault 2024), but they have been collected separately since. RansomLook, used by Müller and Yannikos (2026), could not be reached when we collected the data.

5.2 Cleaning

We dropped 215 records without a date or group and 94 records whose discovery date fell outside the window. Group names were normalised so that versions of the same brand count as one firm (for example lockbit2, lockbit3 and lockbit5 as *lockbit*; blackcat as *alphv*). Brands that were renamed by the same operators are kept separate in the main analysis, because a rebrand is itself a market event. As a robustness check we merge them into *organisations*, using two definitions. The strict definition merges rebrands reported with high confidence by government agencies or threat-intelligence firms: Royal and BlackSuit (CISA and FBI 2024), Cyclops and Knight (Symantec 2024), Eldorado and BlackLock (Mascellino 2025) and Hunters International and World Leaks (Group-IB 2025). The broad definition adds links made with moderate confidence or through code purchases: BlackSuit and Chaos (Cisco Talos 2025), Hive and Hunters International (Group-IB 2025), Knight and RansomHub (Symantec 2024), and INC, Lynx and Sinobi (Unit 42 2024; Blackpoint Cyber 2026). We do not

merge groups that split from one organisation into several, such as the successors of Conti. Each victim received a key: its domain when the domain is specific, otherwise its normalised name. Generic domains (such as gov.br) and placeholder posts ("this entry has been removed") were given unique keys so that they cannot be merged. We removed 614 repeated posts of the same victim by the same group, keeping the first. The final dataset contains **29,162 claims by 287 groups**.

Some victims appear on more than one leak site: 6.8% of claims concern a victim claimed by two or more groups, and 3.5% of claims repeat a victim already claimed by another group. These cross-group repeats are partly re-extortion and partly the republication of stolen data by groups that did not carry out the attack. We flag the earliest claim of every victim as its *first claim* and use first claims as a robustness check throughout.

Country is missing for 81% of claims in 2022 and 55% in 2023, but for at most 6.5% from 2024 onwards. Sector is missing for 12% of claims in 2022 and at most 6.5% afterwards. Geographic results therefore use 2024–2026 only.

5.3 Market concentration (RQ1)

For each quarter we compute each group's share of claims, s_{i}, and the Herfindahl–Hirschman Index:

$$\mathrm{HHI}_t = 10{,}000 \sum_{i=1}^{N_t} s_{it}^2$$

HHI ranges from near 0 (many small firms) to 10,000 (monopoly), and 10,000/HHI gives the number of equal-sized firms that would yield the same concentration. As a reference, the 2023 U.S. Merger Guidelines treat markets with HHI above 1,800 as highly concentrated (U.S. Department of Justice and Federal Trade Commission 2023). We also report the share of the largest group (CR1) and of the five largest (CR5). The trend is estimated by regressing log HHI on a quarterly time index, with Newey–West standard errors (Newey and West 1987). Five robustness checks recompute HHI using first claims only, groups with at least 50 claims only, excluding Clop, whose activity comes in large bursts (for example, 334 claims in February 2025 alone), merging rebrands into organisations, and on the ransomwatch data. For comparison with Müller and Yannikos (2026), we also report the concentration ratio CR_{k} of the top 1%, 5%, 10% and 20% of groups, over the whole period and for each year.

5.4 Brand dynamics (RQ2)

A brand *enters* at its first post and *exits* if it has not posted in the 90 days before the end of observation (30 September 2026). We keep brands with at least three claims and exclude the 17 brands already active in January 2022, whose start is unobserved (left truncation). Active brands are right-censored. We estimate survival with the Kaplan–Meier estimator (Kaplan and Meier 1958) and compare brands that entered in 2022–2023 with those that entered in 2024–2026 using a log-rank test. We also compute, for each year, the share of claims made by brands less than 12 months old. Because the exit rule and the minimum size are arbitrary, we repeat the estimates

with exit thresholds of 60 and 180 days, with minimum sizes of five and ten claims, and at the level of organisations.

5.5 Law-enforcement disruption (RQ3)

Operation Cronos took control of LockBit's infrastructure on 19–20 February 2024 (National Crime Agency 2024; Boyton 2024). We describe LockBit's monthly claims and market share over the 12 months before and after, and compare each group's share of first claims in the six months before and after the operation.

A single operation in a volatile series cannot identify an effect on aggregate activity. An interrupted time series around Operation Cronos alone (Bernal et al. 2017) finds a significant break at a placebo date six months earlier, driven by a burst of ALPHV claims in July 2023. We therefore pool seven operations that disrupted a ransomware group's leak site between 2023 and 2025: Hive (26 January 2023; U.S. Department of Justice 2023a), RagnarLocker (19 October 2023; Eurojust 2023), ALPHV/BlackCat (19 December 2023; U.S. Department of Justice 2023b), LockBit (20 February 2024), Dispossessor (12 August 2024; Help Net Security 2024), 8Base (10 February 2025; Europol 2025) and BlackSuit (24 July 2025; U.S. Department of Justice 2025). For each operation and outcome we compute the difference between the mean of months $+1$ to $+6$ and the mean of months -6 to -1, leaving out the month of the operation. The outcomes are the log of monthly claims by all groups, the same excluding Clop, the log of the number of active groups, and the share of the gains in first-claim market share that went to brands created less than six months before the operation. Because claims grow over the period, the relevant comparison is not zero but the same difference computed around ordinary months. We use randomisation inference: we compare the mean difference across the seven operations with the distribution of the mean across 20,000 random draws of seven months without an operation, among the 38 months with complete windows.

5.6 Specialisation and geography (RQ4)

For the 86 groups with at least 50 claims of known sector, we compare the group's sector mix with the market mix using the Jensen–Shannon divergence (Lin 1991). With base-2 logarithms it ranges from 0 (same mix as the market) to 1 (no overlap). We use the twelve most common sectors plus a residual category. Because the divergence of small samples is biased upwards, we also report its correlation with group size. Geographic shares are computed for 2024–2026, with EU membership defined as the 27 member states.

5.7 Software and use of AI tools

All analyses were run in Python (pandas, statsmodels, lifelines, SciPy). The data were downloaded twice, on the same day, and the two downloads gave identical results. The download and analysis code and the aggregated tables are available in an anonymised public repository (https://github.com/papercaas/CaaS). A large language model (Claude, Anthropic) was used to help write the data-processing code and to draft

parts of the text. The authors designed the study, checked every result against the data and are responsible for the content.

6 Results

6.1 Overview

Visible ransomware activity grew while the number of brands grew faster. Annual claims rose from 2,788 in 2022 to 7,974 in 2025, and 7,493 claims were posted in the first nine months of 2026. The number of groups posting at least once in a year rose from 59 to 144 over the same period (Table 2). Monthly claims rose from about 200 in early 2022 to between 700 and 1,100 in mid-2026 (Fig. 2). Part of this growth reflects wider coverage by the aggregator, which is why the analysis below relies on shares rather than counts. The series is punctuated by bursts from single groups: ALPHV posted 408 victims in July 2023, and Clop 334 in February 2025.

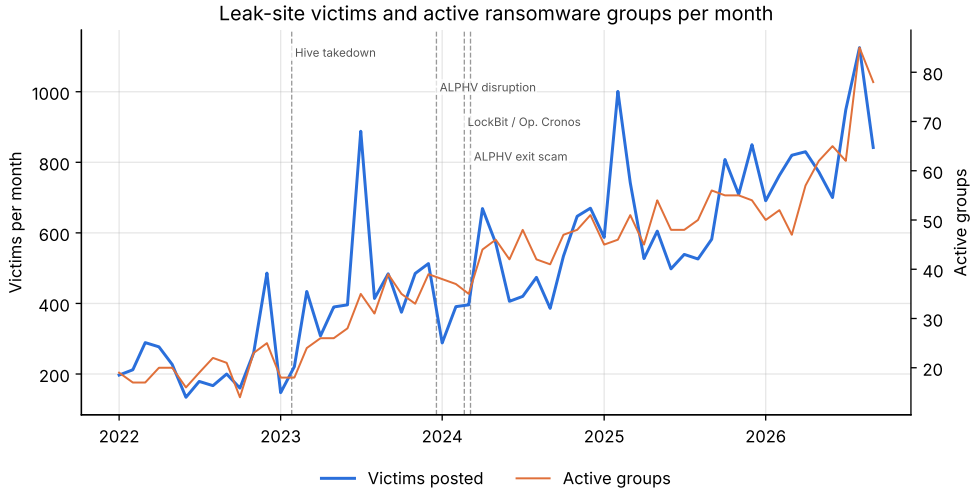


Fig. 2 Monthly leak-site claims and number of active groups, January 2022–September 2026. Dashed lines mark law-enforcement and market events

6.2 Concentration (RQ1)

The RaaS market moved from oligopoly to fragmentation (Fig. 3). In the first three quarters of 2022, the quarterly HHI was between 2,014 and 2,351, above the 1,800 threshold for a highly concentrated market. LockBit alone posted 40–46% of all claims, and the five largest groups 71–75%. From 2024 onwards, HHI stayed between 443 and 734, CR1 between 13% and 20%, and CR5 between 36% and 48%. The equivalent number of equal-sized groups rose from 4–5 to 14–23, and the number of groups active in a quarter from 26 to 107. Log HHI declined by 8.3% per quarter, or about 28%

per year (Newey–West $p < 0.001$, 19 quarters). The decline began before Operation Cronos: HHI had already fallen to 717 in the last quarter of 2023.

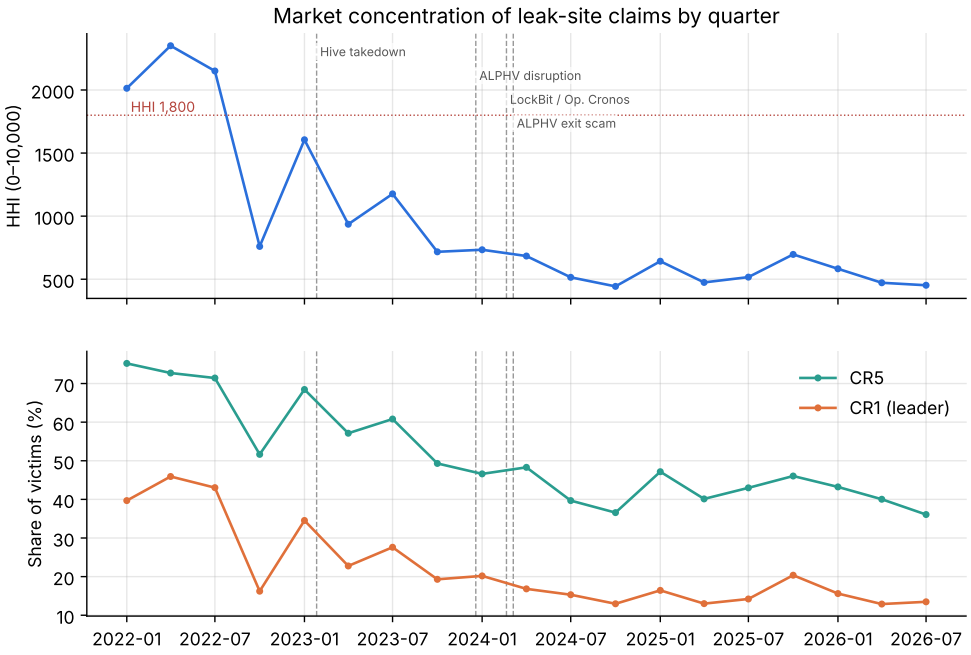


Fig. 3 Quarterly market concentration of leak-site claims. Top: Herfindahl–Hirschman Index; the dotted line marks the 1,800 threshold for highly concentrated markets. Bottom: shares of the largest group (CR1) and the five largest (CR5)

The result is robust to the three alternative samples (Table 2, last columns). Average HHI fell from 1,464 in 2022–2023 to 565 in 2024–2026 in the full sample. It fell from 1,475 to 560 using first claims only, from 1,803 to 688 using only groups with at least 50 claims, and from 1,534 to 567 excluding Clop. Restricting to large groups raises the level of HHI but not the size of the decline, so fragmentation is not an artefact of the aggregator adding small groups. Only one quarter is sensitive to the cleaning: in 2024Q2, Dispossessor appears as the market leader in raw claims. Using first claims, that quarter's HHI drops from 684 to 559, because 88% of Dispossessor's posts repeated victims already claimed by other groups.

Fragmentation is not an artefact of rebranding. Merging documented rebrands into organisations leaves average HHI at 1,464 in 2022–2023 and 565 in 2024–2026 under the strict definition, and 599 under the broad one, with a decline of 27–28% per year in both cases. Nor is it specific to one aggregator. In 2022–2024, ransomwatch records 12,484 claims by 132 groups, against 13,695 claims by 149 groups in our data. 75% of our claims appear in ransomwatch under the same group, and quarterly HHI in the two sources is highly correlated (Pearson $r = 0.96$). The two sources identify the same

leader in 10 of 12 quarters, and ransomwatch shows the same decline, of 34% per year against 43% in our data over the same window (both $p < 0.001$; Online Resource 1).

Our data reproduce the static picture of Müller and Yannikos (2026). Over the whole period, the top 1% of groups (3 groups) account for 23.3% of claims, the top 5% (14 groups) for 53.2%, the top 10% (29) for 67.5% and the top 20% (57) for 81.6%, against 21.3%, 51.8%, 67.5% and 82.7% in their data. Thirteen groups account for half of all claims. The period average, however, hides the trend: the share of the three largest groups fell from 46.3% in 2022 and 40.0% in 2023 to 25.4% in 2024, 28.4% in 2025 and 29.8% in 2026.

Table 2 Market structure by year

Year	Claims	Active groups	Groups for 50% of claims	HHI	Largest group (share)	Mean quarterly HHI, first claims only
2022	2,788	59	4	1,380	LockBit (34.1%)	1,830
2023	5,055	69	5	783	LockBit (20.6%)	1,120
2024	5,852	95	10	396	RansomHub (10.2%)	566
2025	7,974	123	9	436	Qilin (13.0%)	593
2026 (Jan–Sep)	7,493	144	9	447	Qilin (13.5%)	510

Annual HHI is lower than the quarterly average because leadership rotates within a year. Leadership changed hands repeatedly after 2023: LockBit led until early 2024, RansomHub in the second half of 2024, Clop in early 2025, Qilin from the second quarter of 2025 and The Gentlemen in the third quarter of 2026 (Fig. 4). By 2024, ten groups were needed to account for half of all claims, against four in 2022. These findings support E1.

6.3 Brand turnover (RQ2)

Brands are short-lived. Of the 239 brands that entered the market after January 2022 and posted at least three claims, 141 had stopped posting by the end of the observation period. The Kaplan–Meier median lifetime is 9.1 months (95% CI 5.7–15.4), and fewer than half of brands are still active 12 months after their first post (Fig. 5). The exact figure depends on the definitions (Table 3). With exit thresholds of 60 and 180 days the median is 8.8 and 13.6 months. Larger brands live longer: the median is 11.4 months for brands with at least five claims and 19.2 months for those with at least ten. Merging rebrands changes little (9.4 months under the strict definition, 9.1 under the broad one). Brands that entered in 2024–2026 do not live shorter lives than those that entered in 2022–2023 (median 8.8 vs 9.4 months; 46% vs 47% active after 12 months; log-rank $p = 0.56$). This holds in all fifteen specifications (log-rank p between 0.10 and 0.85). The market fragmented through more entry, not faster exit.

Brands entering after January 2022 only; n = 239 brands (230–235 organisations) with at least three claims, 216 with at least five, 174 with at least ten.

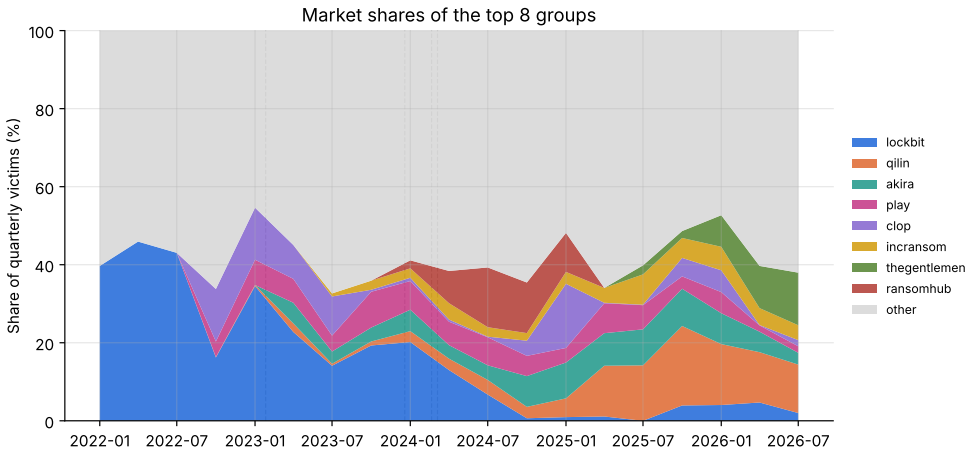


Fig. 4 Quarterly shares of the eight groups with the most claims over the whole period. Grey: all other groups

Table 3 Sensitivity of brand survival to the definition of exit and of a brand (Kaplan–Meier median lifetime in months, 95% CI in brackets)

Unit	Minimum claims	Exit after 60 days	Exit after 90 days	Exit after 180 days
Brand	3	8.8 (5.5–14.5)	9.1 (5.7–15.4)	13.6 (7.8–19.7)
Brand	5	10.1 (7.3–17.6)	11.4 (7.6–19.2)	15.4 (8.4–20.3)
Brand	10	17.6 (10.1–20.4)	19.2 (11.4–23.7)	20.3 (14.9–29.0)
Organisation, strict	3	9.1 (5.7–14.9)	9.4 (6.3–15.5)	14.5 (8.1–20.3)
Organisation, broad	3	9.1 (5.5–15.4)	9.1 (5.7–17.6)	14.5 (7.8–20.3)

New brands carry a large part of the market. Brands less than 12 months old produced 56% of claims in 2023, 53% in 2024, 40% in 2025 and 43% in 2026. This supports E2: a brand behaves like a storefront that can be opened and closed, while affiliates and their access persist.

6.4 Law-enforcement disruption (RQ3)

Operation Cronos ended LockBit's leadership, but not immediately (Fig. 6). In the six months before February 2024, LockBit posted 88 claims per month on average, 20.7% of the market. In months 1–6 after the operation it still posted 57 per month (11.7%), with a peak of 176 claims in May 2024. In months 7–12 it posted 7 per month, 1.0% of the market. Industry analysis found that many post-takedown LockBit posts were reuploads of attacks that predated the operation (Boyton 2024). Our deduplication removes exact repeats only, so the post-takedown figures are an upper bound on new LockBit activity.

LockBit's lost share went mostly to new brands (Fig. 7). Comparing first claims in the six months before and after the operation, LockBit lost 8.5 percentage points

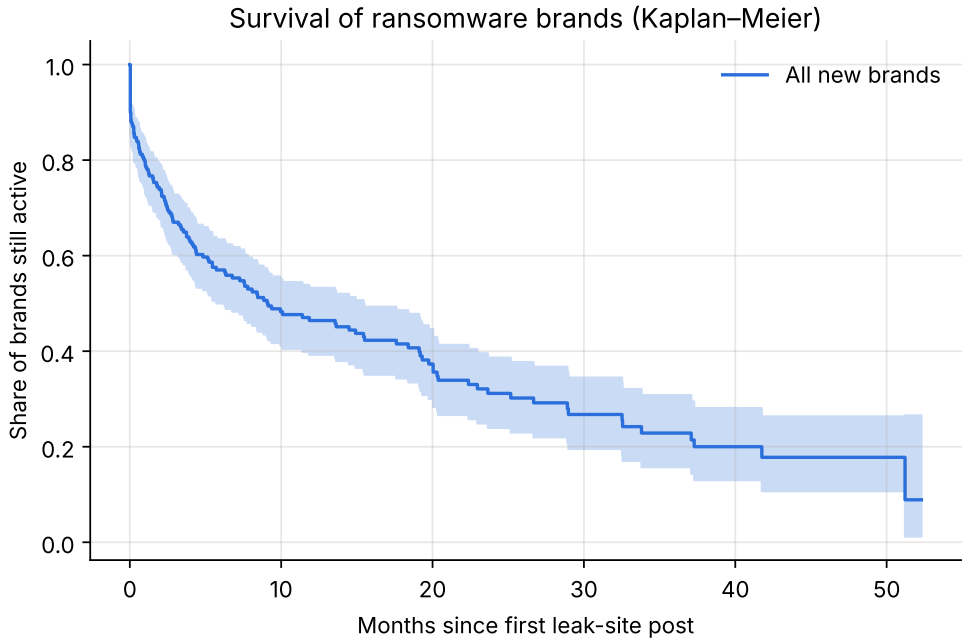


Fig. 5 Kaplan–Meier survival of ransomware brands that entered after January 2022 (≥3 claims; exit = no post in the last 90 days). Shaded area: 95% confidence interval

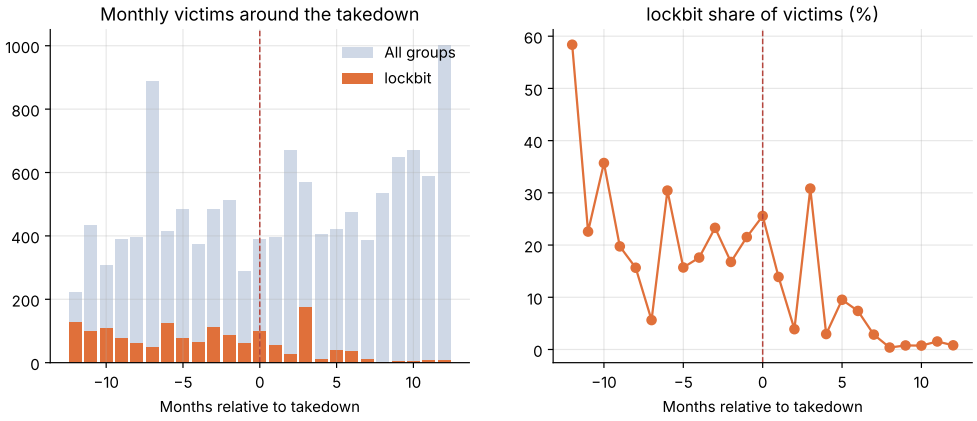


Fig. 6 Monthly claims (left) and LockBit's share of claims (right) in the 12 months before and after Operation Cronos (month 0 = February 2024)

and ALPHV, which left the market through an exit scam in 2024 (Toulas 2025), lost 7.9. The largest gain went to RansomHub (+10.5 points), whose first post appeared ten days before Operation Cronos. Smaller gains went to established groups such as

BlackSuit (+2.5), Hunters International (+2.4) and Qilin (+2.0). Overall, brands created less than six months before the operation captured 77% of all share gains. The pattern repeated a year later: when RansomHub went offline in April 2025 (Lakshmanan 2025), Qilin's quarterly share rose from 4.8% to 13.0% and reached 20.4% by the end of 2025.

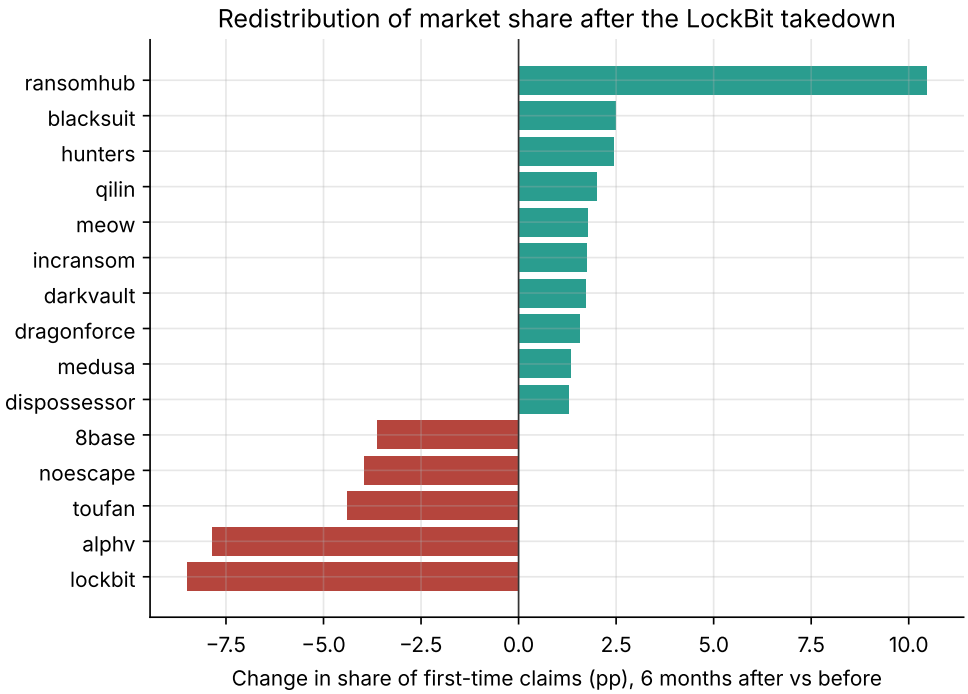


Fig. 7 Change in each group's share of first claims, six months after versus six months before Operation Cronos (percentage points). The five largest losses and ten largest gains are shown

The same pattern appears across all seven operations (Table 4). In six of the seven cases the targeted group's share of claims fell to zero or close to it within six months; LockBit took a year. The rest of the market did not shrink. On average, log monthly claims were 0.14 higher in the six months after an operation than in the six months before. Around ordinary months the same difference is 0.22, reflecting the growth of the series, and the gap is well within the range expected by chance (randomisation $p = 0.27$; 0.28 excluding Clop). The number of active groups was also unaffected ($p = 0.68$), and Fig. 8 shows no break in the average path of claims around the operations. Who gained the lost share was not specific to the operations either. Brands created less than six months earlier captured on average 69% of share gains after an operation, against 71% around ordinary months ($p = 0.62$). Redistribution to new brands is therefore not a response to disruption but the normal way this market renews itself, which a takedown leaves intact.

Table 4 Seven law-enforcement operations against ransomware groups: targeted group and market, six months after versus six months before

Operation	Date	Target share of claims, before → after	Change in log market claims	Share of gains to new brands
Hive	26 Jan 2023	5.3% → 0.0%	+0.59	62%
RagnarLocker	19 Oct 2023	0.7% → 0.0%	−0.02	73%
ALPHV/BlackCat	19 Dec 2023	18.6% → 2.0%	−0.10	64%
LockBit (Cronos)	20 Feb 2024	20.7% → 11.7%	+0.14	77%
Dispossessor	12 Aug 2024	10.0% → 0.0%	+0.28	56%
8Base	10 Feb 2025	1.5% → 0.0%	+0.05	66%
BlackSuit	24 Jul 2025	0.2% → 0.0%	+0.07	62%
Mean			**+0.14**	**69%**
Ordinary months			+0.22 ($p = 0.27$)	71% ($p = 0.62$)

Months −6 to −1 versus +1 to +6; the month of the operation is excluded. New brands: first post less than six months before the operation. p-values from randomisation inference over 38 months without an operation. BlackSuit had largely stopped posting before the operation, after the emergence of Chaos.

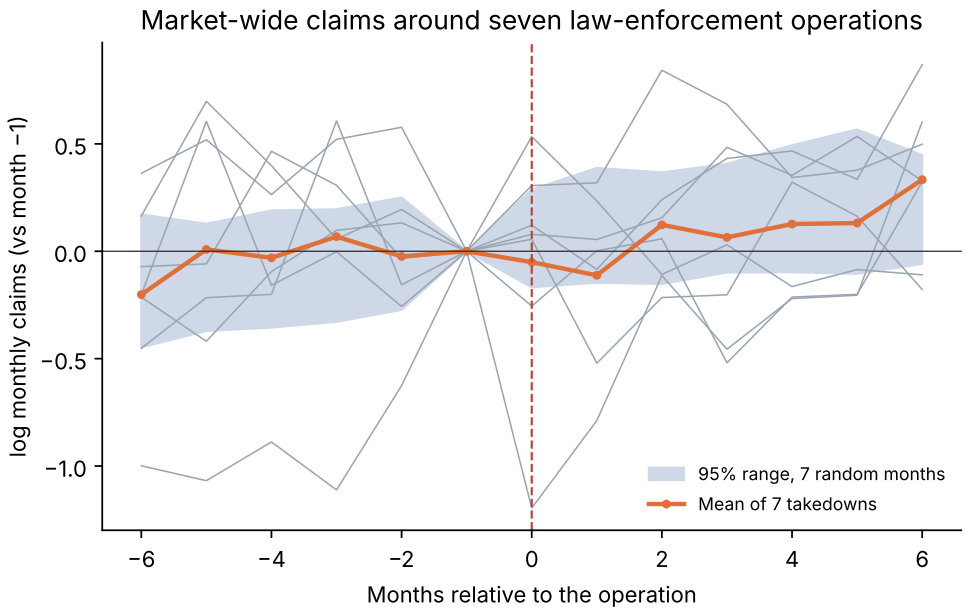


Fig. 8 Log monthly leak-site claims around seven law-enforcement operations, relative to the month before the operation. Grey lines: individual operations; orange: their mean; shaded area: 95% range of the mean for seven randomly chosen months without an operation

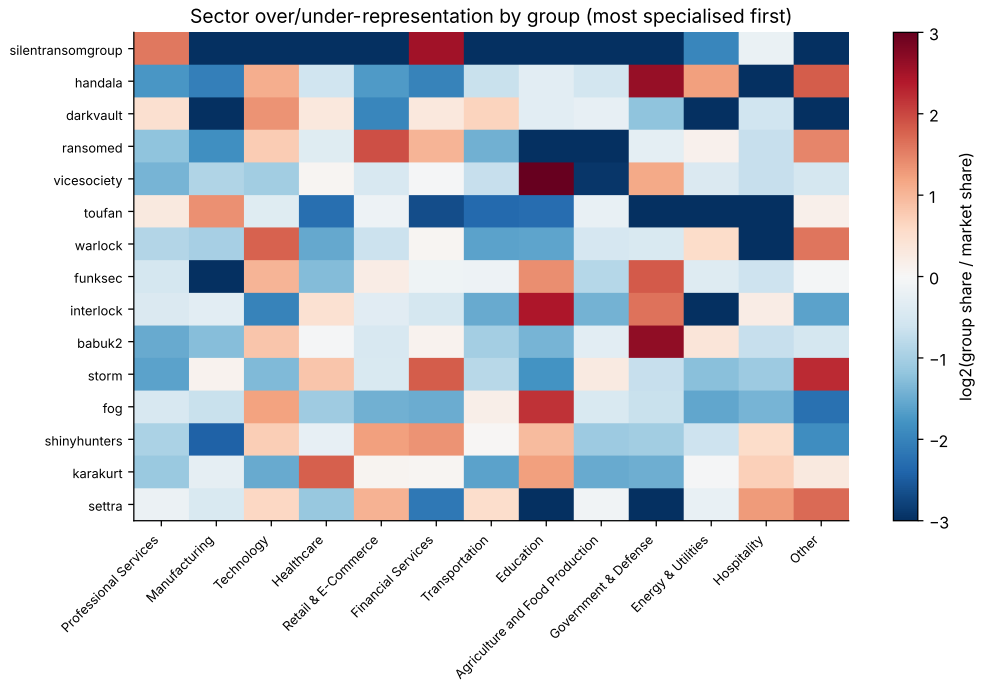


Fig. 9 Sector over- and under-representation for the fifteen most specialised groups ($\log_2$ ratio of the group's sector share to the market's sector share; red = over-represented)

For LockBit alone, an interrupted time series of log monthly claims gives a level change of -0.19 ($p = 0.37$) and a slope change of $+0.02$ ($p = 0.42$) at the operation, but the same model finds a significant break at a placebo date six months earlier (-0.55, $p = 0.005$). This is why we rely on the pooled comparison above. Taken together, the results show no sustained fall in visible activity after any of the operations, consistent with E3.

6.5 Specialisation and geography (RQ4)

Most groups are generalists. Over the whole period, professional services account for 20.0% of claims with a known sector, manufacturing 18.5%, technology 13.1% and healthcare 8.9%. Among the 86 groups with at least 50 claims of known sector, the median Jensen–Shannon divergence from this mix is 0.21 (interquartile range 0.17–0.28). The largest programmes are the least specialised: Qilin (0.06), LockBit (0.07), The Gentlemen (0.11) and ALPHV (0.12) mirror the market almost exactly. The most specialised groups are small (Fig. 9). Silent Ransom Group directs 59% of its claims at professional services, Vice Society 37% at education and Toufan 48% at manufacturing. Size and divergence are negatively correlated (Spearman $\rho = -0.43$, $p < 0.001$). Part of this correlation is the small-sample bias of the divergence, but it is also what one would expect if large RaaS programmes are platforms whose many affiliates each pick their own targets.

In 2024–2026, when country information is nearly complete, the United States accounts for 46.5% of claims and the EU-27 for 18.1%, rising from 16.9% in 2024 to 20.2% in 2026 (Table 5). Within the EU, Germany accounts for 25.3% of claims, Italy 15.4%, France 14.0% and Spain 11.7%. Italy ranks fifth worldwide and second in the EU, with 154 claims in 2024, 176 in 2025 and 231 in the first nine months of 2026. Italian victims are more often manufacturers than victims elsewhere (27.6% versus 18.0% of claims). The five groups most active in Italy (Qilin, LockBit, The Gentlemen, Akira and RansomHub) account for 37% of Italian claims.

Table 5 Countries with the most claims, 2024–September 2026 (n = 20,093 claims with known country)

Rank	Country	Claims	Share	EU
1	United States	9,342	46.5%	
2	Germany	921	4.6%	✓
3	Canada	909	4.5%	
4	United Kingdom	881	4.4%	
5	Italy	561	2.8%	✓
6	France	510	2.5%	✓
7	Brazil	452	2.2%	
8	India	447	2.2%	
9	Spain	428	2.1%	✓
10	Australia	378	1.9%	

7 Discussion

7.1 A contestable market

The three expectations derived from the supply-chain model all hold. Concentration fell steadily and is now far below any threshold of market power (E1). Brands are short-lived, and new brands produce up to half of all claims (E2). The removal of the dominant brand shifted its share to rivals and newcomers without a visible fall in activity, and the same holds across seven operations (E3).

In industrial-organisation terms, RaaS behaves like a contestable market. Entry is cheap because the inputs that matter most are mobile: affiliates, access bought from brokers, and code that can be forked or rebranded. Exit is cheap for the same reason. A brand is closer to a storefront than to a firm, and the people behind it can reopen elsewhere. This reading fits evidence from other illicit online markets, where the effects of police operations were often short-lived (Collier et al. 2019) and part of the trade was displaced to other markets (Décary-Hétu and Giommoni 2017). It also refines the common description of the ecosystem as "dominated by a few actors". That description was accurate for 2022 but no longer holds. It also persists because static measures over long periods, such as the share of the top 5% of groups, mix the concentrated market of 2022 with the fragmented market that followed.

Fragmentation is not only good news for criminals. Smaller, newer brands have less reputation to protect, and the 2024 exit scam of ALPHV shows that trust between operators and affiliates is fragile (Toulas 2025). Ransom payments fell by about 35% in 2024 while leak-site claims rose (Toulas 2025). Our data cannot establish a link, but the combination is consistent with a market in which more brands compete for victims who pay less often.

For the debate on whether ransomware groups are organised crime (Leukfeldt et al. 2017; Whelan et al. 2024), the results separate two levels. Inside the largest groups, studies of Conti find firm-like hierarchies and human-resources practices (Paternoster et al. 2025; Martin et al. 2025). At the level of the market, however, no group has exercised the lasting market control associated with stricter definitions of organised crime since 2022. Large organisations exist, but they operate in a market that none of them controls.

7.2 Implications for law enforcement

If brands are cheap to replace, removing a brand buys time rather than market share. Across seven operations, the targeted brands lost almost all of their market share, but the market did not shrink. Operation Cronos ended LockBit's leadership within a year, and the operation's other effects (seized keys, identified affiliates, damage to LockBit's reputation) are not visible in our data. But the market as a whole did not shrink. Interventions are likely to have more lasting effects where inputs are scarce and shared across brands: initial access brokers, infostealer infrastructure, laundering services and the individual affiliates who move from one programme to the next. Market-structure indicators such as HHI, entry rates and brand survival could be tracked routinely to evaluate interventions, alongside the counts of victims that are reported today.

7.3 Implications for organisations

For defenders, the lesson of fragmentation is to defend against techniques rather than brands. A shrinking share of attacks comes from any single group, and brand names change every few months, but the techniques in Table 1 change slowly. Four measures cover most of the chain. Phishing-resistant MFA and monitoring of session tokens address the PhaaS techniques that feed initial access. Rapid patching of edge devices and remote services reduces what brokers can sell. Allow-listing of remote management tools and monitoring of large outbound transfers make lateral movement and exfiltration visible. Offline or immutable backups, tested regularly, limit the leverage of encryption, though not of data theft.

The supply-chain view extends to suppliers. Contracts with managed service providers and software vendors should limit privileged access to what is needed, require prompt notification of incidents and vulnerabilities, and, for software, require a software bill of materials. In the EU, these obligations are now partly mandatory. The NIS2 Directive imposes risk-management and incident-reporting duties on essential and important entities (European Parliament and Council 2022). The Cyber Resilience Act sets security requirements for products with digital elements, including

vulnerability handling over the product's life cycle (European Parliament and Council 2024).

For Italy, the data point to a specific exposure. Italy is the second most targeted EU country, its claims rose every year in our window, and its victims are disproportionately manufacturers. Supplier security and sector-level information sharing are therefore particularly relevant for Italian manufacturing. Our data do not record firm size, so whether small and medium-sized firms are over-represented remains an open question.

7.4 Implications for threat-intelligence measurement

Leak-site data are increasingly used to rank groups and track trends, often without cleaning. Our results show that cleaning changes conclusions at the margin. Without it, a group that mostly republished other groups' victims would appear as the market leader in one quarter. Reports based on these data should deduplicate across groups, normalise brand names and distinguish first claims from reposts, and they should report shares and concentration alongside raw counts, which are sensitive to changes in coverage.

8 Limitations and future work

Our data measure claims, not attacks or revenues. Victims who pay are usually never posted, so a group with a high payment rate appears smaller than it is. Market shares based on claims may therefore differ from shares based on ransom income, which would require blockchain data such as those of Cable et al. (2024). Groups may also post false claims or inflate their lists to attract affiliates.

Coverage changes over time. ransomware.live has added leak sites as new groups appeared, and its early records lack country information. We rely on shares rather than counts, show that results hold among groups with at least 50 claims and in a second tracker, and restrict geography to 2024–2026. The second tracker is not fully independent of ours and covers only 2022–2024, and RansomLook could not be included. Still, if the aggregator added small groups faster than they actually appeared, the count of active groups would overstate fragmentation. HHI is much less sensitive to this, because small groups contribute little to it.

Brand names are an imperfect unit. Rebrands count as new entrants, and splinter groups that keep an old name count as continuations. Merging documented rebrands does not change our conclusions, but attribution of rebrands rests on public threat-intelligence reporting, which is incomplete and sometimes contested. Linking brands systematically through shared code, infrastructure or affiliates would allow concentration to be measured at the level of the people behind the brands, which may be higher.

The event study pools seven operations, but their windows partly overlap (ALPHV and LockBit) and their targets differed greatly in size, so the comparison has limited power to detect small effects. It shows the absence of a large market-wide effect, not a precise estimate. Synthetic controls built from unaffected groups, or data on affiliates

moving between programmes, would allow sharper tests. Finally, the analysis ends in September 2026, and the most recent quarters may be revised as late posts are added.

9 Conclusion

Cybercrime-as-a-Service is often described as an industry. Treating it as one, with the standard tools of market analysis, gives a clear answer about its recent evolution. Between 2022 and 2026, the ransomware market moved from a tight oligopoly led by LockBit to a fragmented market of more than a hundred short-lived brands, with no single group holding more than 21% of quarterly claims since 2024. The takedown of the market leader ended its dominance but did not reduce visible activity, and the same holds across seven law-enforcement operations between 2023 and 2025. The share lost by targeted groups passed to rivals and new brands in the same way as in ordinary months, and the same happened when RansomHub disappeared in 2025.

For law enforcement, this argues for targeting the scarce inputs shared across brands, such as access brokers, infostealers, laundering services and affiliates, and for measuring success by the structure of the market as well as by the fate of individual groups. For organisations, it argues for defences organised around techniques rather than threat-actor names. For researchers, it shows that leak-site data can support economic analysis, provided they are cleaned for reposts and read as shares rather than counts.

References

Akyazi U, van Eeten M, Hernández Gañán C (2021) Measuring Cybercrime as a Service (CaaS) offerings in a cybercrime forum. Workshop on the Economics of Information Security (WEIS 2021). https://weis2021.econinfosec.org/wp-content/uploads/sites/9/2021/06/weis21-akyazi.pdf

Bernal JL, Cummins S, Gasparrini A (2017) Interrupted time series regression for the evaluation of public health interventions: a tutorial. Int J Epidemiol 46(1):348–355. https://doi.org/10.1093/ije/dyw098

Blackpoint Cyber (2026) Sinobi ransomware. Threat profile, February 2026. https://blackpointcyber.com/wp-content/uploads/2026/02/Sinobi.pdf

Boyton C (2024) Unveiling the fallout: Operation Cronos' impact on LockBit following landmark disruption. Trend Micro Research, 3 April 2024. https://trendmicro.com/en_in/research/24/d/operation-cronos-aftermath.html

Cable J, Gray IW, McCoy D (2024) Showing the receipts: understanding the modern ransomware ecosystem. In: 2024 APWG Symposium on Electronic Crime Research (eCrime). IEEE, pp 149–161. https://doi.org/10.1109/eCrime66200.2024.00017

CISA, FBI (2024) #StopRansomware: BlackSuit (Royal) ransomware. Cybersecurity Advisory AA23-061A, updated 7 August 2024. https://www.cisa.gov/news-event

s/cybersecurity-advisories/aa23-061a

Cisco Talos (2025) Unmasking the new Chaos RaaS group attacks. Cisco Talos Blog, 24 July 2025. https://blog.talosintelligence.com/new-chaos-ransomware/

Collier B, Thomas DR, Clayton R, Hutchings A (2019) Booting the booters: evaluating the effects of police interventions in the market for denial-of-service attacks. In: Proceedings of the Internet Measurement Conference (IMC '19). ACM, pp 50–64. https://doi.org/10.1145/3355369.3355592

Décary-Hétu D, Giommoni L (2017) Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of Operation Onymous. Crime Law Soc Change 67(1):55–75. https://doi.org/10.1007/s10611-016-9644-4

Di Nicola A, Baratto G, Vettori B (2025) Criminological definitions of organized crime on the digital test bench: towards a physical–digital framework. Trends Organ Crime (online first). https://doi.org/10.1007/s12117-025-09575-3

Eurojust (2023) Major international operation against the Ragnar Locker ransomware group with Eurojust support. Press release, 20 October 2023. https://www.eurojust.europa.eu/news/major-international-operation-against-ragnar-locker-ransomware-group-eurojust-support

European Parliament and Council (2022) Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive). OJ L 333, 27.12.2022, pp 80–152. http://data.europa.eu/eli/dir/2022/2555/oj

European Parliament and Council (2024) Regulation (EU) 2024/2847 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act). OJ L, 2024/2847, 20.11.2024. http://data.europa.eu/eli/reg/2024/2847/oj

Europol (2025) Key figures behind Phobos and 8Base ransomware arrested in international cybercrime crackdown. Press release, 11 February 2025. https://www.europol.europa.eu/media-press/newsroom/news/key-figures-behind-phobos-and-8base-ransomware-arrested-in-international-cybercrime-crackdown

Group-IB (2025) The beginning of the end: the story of Hunters International. Group-IB Blog, 2 April 2025. https://www.group-ib.com/blog/hunters-international-ransomware-group/

Help Net Security (2024) International investigation shuts down Radar/Dispossessor ransomware group. 13 August 2024. https://www.helpnetsecurity.com/2024/08/13/radar-dispossessor-disruption/

Highet J (2025) ransomwatch: posts.json. GitHub repository joshhighet/ransomwatch. https://github.com/joshhighet/ransomwatch

Huang K, Siegel M, Madnick S (2018) Systematically understanding the cyber attack business: a survey. ACM Comput Surv 51(4):1–36. https://doi.org/10.1145/3199674

Kaplan EL, Meier P (1958) Nonparametric estimation from incomplete observations. J Am Stat Assoc 53(282):457–481

Kool HM, Moneva A, Leukfeldt R (2026) Exploring trust signals and pathways on cybercrime-as-a-service markets: the case of remote access trojans. Trends Organ Crime (online first). https://doi.org/10.1007/s12117-026-09606-7

Lakshmanan R (2025) RansomHub went dark April 1; affiliates fled to Qilin, DragonForce claimed control. The Hacker News, 30 April 2025. https://thehackernews.com/2025/04/ransomhub-went-dark-april-1-affiliates.html

Leukfeldt ER, Lavorgna A, Kleemans ER (2017) Organised cybercrime or cybercrime that is organised? An assessment of the conceptualisation of financial cybercrime as organised crime. Eur J Crim Policy Res 23(3):287–300. https://doi.org/10.1007/s10610-016-9332-z

Lin J (1991) Divergence measures based on the Shannon entropy. IEEE Trans Inf Theory 37(1):145–151

Lusthaus J, Kleemans E, Leukfeldt R, Levi M, Holt T (2024) Cybercriminal networks in the UK and beyond: network structure, criminal cooperation and external interactions. Trends Organ Crime 27(3):364–387. https://doi.org/10.1007/s12117-022-09476-9

Martin J, Whelan C, Bright D (2025) Ransomware HR: human resources practices and organizational support in the Conti ransomware group. Deviant Behav 46(9):1088–1103. https://doi.org/10.1080/01639625.2024.2419905

Mascellino A (2025) Researchers confirm BlackLock as Eldorado rebrand. Infosecurity Magazine, 17 March 2025. https://www.infosecurity-magazine.com/news/researchers-confirm-blacklock

Matthijsse SR, van 't Hoff-de Goede MS, Leukfeldt ER (2023) Your files have been encrypted: a crime script analysis of ransomware attacks. Trends Organ Crime (online first). https://doi.org/10.1007/s12117-023-09496-z

Meland PH, Bayoumy YFF, Sindre G (2020) The Ransomware-as-a-Service economy within the darknet. Comput Secur 92:101762. https://doi.org/10.1016/j.cose.2020.101762

Meurs T, Junger M, Cruyff M, van der Heijden PGM (2026) Estimating the number of ransomware attacks. J Quant Criminol 42(2):227–243. https://doi.org/10.1007/s10940-025-09625-7

Microsoft (2025) Microsoft Digital Defense Report 2025: Lighting the path to a secure future. Microsoft Threat Intelligence

Müller L, Yannikos Y (2026) Analyzing concentration, temporal routines and targeting in public ransomware leak site data. arXiv:2605.24559. https://doi.org/10.48550/arXiv.2605.24559

Musotto R, Wall DS (2022) More Amazon than Mafia: analysing a DDoS stresser service as organised cybercrime. Trends Organ Crime 25(2):173–191. https://doi.org/10.1007/s12117-020-09397-5

National Crime Agency (2024) International investigation disrupts the world's most harmful cyber crime group. 20 February 2024. https://www.nationalcrimeagency.gov.uk/news/nca-leads-international-investigation-targeting-worlds-most-harmful-ransomware-group

Nazzari M (2023) From payday to payoff: exploring the money laundering strategies of cybercriminals. Trends Organ Crime (online first). https://doi.org/10.1007/s12117-023-09505-1

Nershi K (2025) Informal allies: state–cybercriminal alignment in the ransomware ecosystem. J Cybersecur 11(1):tyaf037. https://doi.org/10.1093/cybsec/tyaf037

Newey WK, West KD (1987) A simple, positive semi-definite, heteroskedasticity and autocorrelation consistent covariance matrix. Econometrica 55(3):703–708

Paquet-Clouston M, García S (2022) On the motivations and challenges of affiliates involved in cybercrime. Trends Organ Crime (online first). https://doi.org/10.1007/s12117-022-09474-x

Paternoster C, Nazzari M, Jofre M, Uberti TE (2025) Inside the leak: exploring the structure of the Conti ransomware group. Glob Crime 26(2):148–171. https://doi.org/10.1080/17440572.2025.2473350

Phipps A, Nurse JRC (2026) Inside ransomware groups: an analysis of their origins, structures, and dynamics. Comput Secur 160:104705. https://doi.org/10.1016/j.cose.2025.104705

Poireault K (2024) #CyberMonth: Inside Ransomware.live, free ransomware intelligence for everyone. Infosecurity Magazine, 3 October 2024. https://www.infosecurity-magazine.com/interviews/ransomwarelive-intelligence

ransomware.live (2026) Ransomware.live API documentation, version 2. https://www.ransomware.live/apidocs

Ruellan E, Paquet-Clouston M, Garcia S (2024) Conti Inc.: understanding the internal discussions of a large ransomware-as-a-service operator with machine learning.

Crime Sci 13:16. https://doi.org/10.1186/s40163-024-00212-y

Strom BE, Applebaum A, Miller DP, Nickels KC, Pennington AG, Thomas CB (2018) MITRE ATT&CK: design and philosophy. Technical report, The MITRE Corporation, revised March 2020. https://www.mitre.org/news-insights/publication/mitre-attck-design-and-philosophy

Symantec (2024) RansomHub: new ransomware has origins in older Knight. Symantec Enterprise Blog, 5 June 2024. https://www.security.com/threat-intelligence/ransomhub-knight-ransomware

Toulas B (2025) Ransomware payments fell by 35% in 2024, totalling $813,550,000. BleepingComputer, 5 February 2025. https://www.bleepingcomputer.com/news/security/ransomware-payments-fell-by-35-percent-in-2024-totalling-813-550-000/

U.S. Department of Justice (2023a) U.S. Department of Justice disrupts Hive ransomware variant. Press release, 26 January 2023. https://www.justice.gov/archives/opa/pr/us-department-justice-disrupts-hive-ransomware-variant

U.S. Department of Justice (2023b) Justice Department disrupts prolific ALPHV/BlackCat ransomware variant. Press release, 19 December 2023. https://www.justice.gov/usao-sdfl/pr/justice-department-disrupts-prolific-alphvblackcat-ransomware-variant

U.S. Department of Justice (2025) Justice Department announces coordinated disruption actions against BlackSuit (Royal) ransomware operations. Press release, 11 August 2025. https://www.justice.gov/opa/pr/justice-department-announces-coordinated-disruption-actions-against-blacksuit-royal

U.S. Department of Justice, Federal Trade Commission (2023) Merger Guidelines. 18 December 2023

Unit 42 (2024) Lynx ransomware: a rebranding of INC ransomware. Palo Alto Networks, 10 October 2024. https://unit42.paloaltonetworks.com/inc-ransomware-rebrand-to-lynx/

van Wegberg R, Tajalizadehkhoob S, Soska K, Akyazi U, Hernández Gañán C, Klievink B, Christin N, van Eeten M (2018) Plug and prey? Measuring the commoditization of cybercrime via online anonymous markets. In: 27th USENIX Security Symposium. USENIX Association. https://www.usenix.org/conference/usenixsecurity18/presentation/wegberg

Whelan C, Bright D, Martin J (2024) Reconceptualising organised (cyber)crime: the case of ransomware. J Criminol 57(1):45–61. https://doi.org/10.1177/26338076231199793

Whelan C, Jones C, Martin J, Bright DA (2026) The internal structure of ransomware criminal groups: an analysis of organisational units, functions, roles, and communication patterns within Conti. Glob Crime 27(2):112–134. https://doi.org/10.1080/17440572.2025.2534387

Supplementary Files

This is a list of supplementary files associated with this preprint. Click to download.

- ESM1.pdf