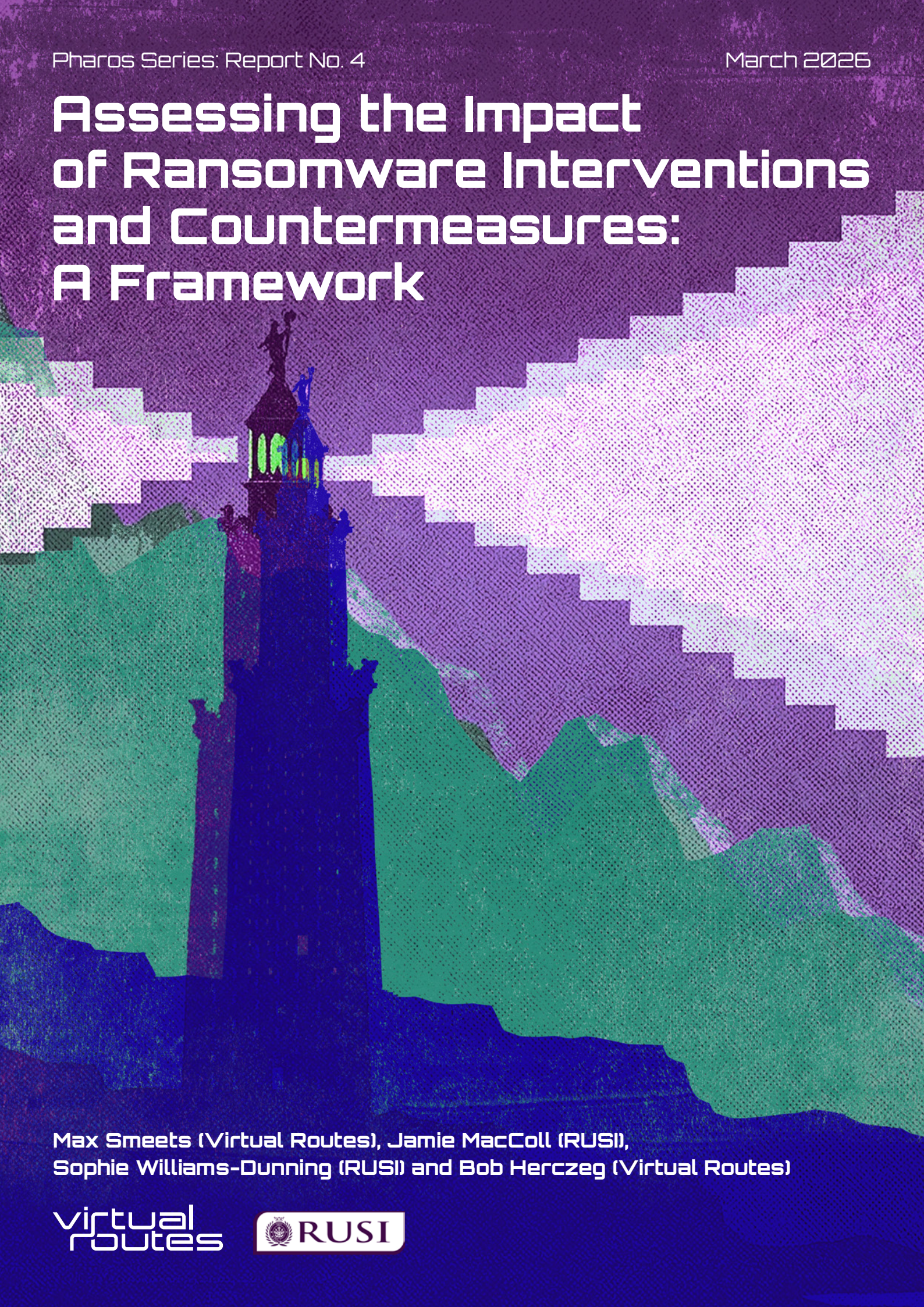
Pharos Series: Report No. 4 March 2026

Assessing the Impact of Ransomware Interventions and Countermeasures: A Framework



Max Smeets (Virtual Routes), Jamie MacColl (RUSI),
Sophie Williams-Dunning (RUSI) and Bob Herczeg (Virtual Routes)

virtual routes

RUSI

PHAROS SERIES

Virtual Routes | www.virtual-routes.org

Design & Layout by Frank Wo | Cover by Vahram Muradyan | Edited by Katharine Khamhaengwong

This project was made possible by the support of the German Federal Foreign Office. The views expressed in this paper do not necessarily represent the views or policies of the ministry or the government.

Assessing the Impact of Ransomware Interventions and Countermeasures: A Framework

Max Smeets (Virtual Routes), Jamie MacColl (RUSI),
Sophie Williams-Dunning (RUSI), and
Bob Herczeg (Virtual Routes)

virtual routes | RUSI

ABOUT THE AUTHORS

Max Smeets

Max Smeets is the Co-Director of Virtual Routes, and serves as Managing Editor of Binding Hook. He also holds research positions at ETH Zurich, the Royal United Services Institute (RUSI) and Stanford University's Center for International Security and Cooperation. Max is the author of Ransom War: How Cyber Crime Became a Threat to National Security and No Shortcuts: Why States Struggle to Develop a Military Cyber Force.

Max received a BA in Economics, Politics and Statistics from University College Roosevelt, Utrecht University and an MPhil (Brasenose College) and DPhil (St. John's College) in International Relations from the University of Oxford.

Jamie MacColl

Jamie MacColl is a Senior Research Fellow in cyber security at the Royal United Services Institute. His current research interests include ransomware, the UK's approach to offensive cyber operations, and the role of private companies in global cyber governance. He has led a range of public and private projects for RUSI, with a particular focus on UK cyber policy. Prior to joining RUSI, he worked in cyber threat intelligence where he provided strategic and operational intelligence analysis on the cyber threat landscape. Jamie is also a Senior Research Associate at Virtual Routes.

Jamie holds an MPhil in International Relations and Politics from the University of Cambridge, where his research focused on UK policy towards Russia since the end of the Cold War. He also holds a BA in War Studies from King's College London, where he was awarded the Sir Michael Howard Excellence Award in 2016 and 2018.

When he is not carrying out research into cyber threats and cyber security, Jamie can be found on stage with his band Bombay Bicycle Club.

Sophie Williams-Dunning

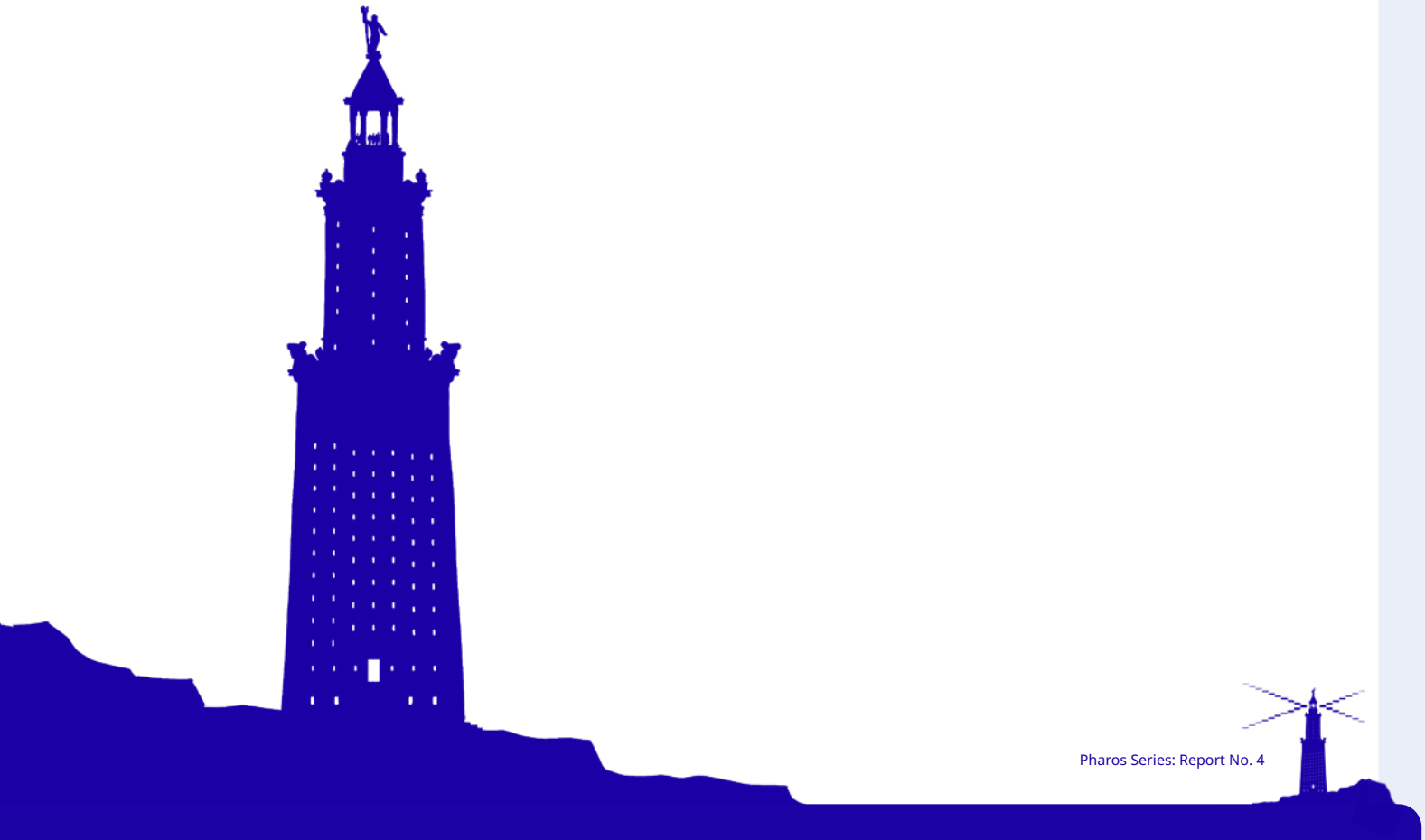
Sophie is a Research Analyst in the Cyber and Tech team. Her research interests include the evolution of hostile state threats in cyber-space and through cyber means, information operations, as well as UK cyber strategy and defence-tech innovation.

Sophie holds an MA with Distinction in Intelligence and International Security from the War Studies Department at King's College London, where she studied foreign policy with a focus on Russia, national cyber strategies, intelligence, and open-source investigation.

Bob Herczeg

Bob Herczeg is an Executive Support and Research Officer at Virtual Routes. He holds a Bachelor of Arts (Hons) degree in War Studies from King's College London and is an Associate of King's College. His research interests include cyber conflict, cybersecurity for maritime critical infrastructure, and grey zone operations in the Baltic and South China Seas. He has been a producer and researcher for lauded short-form documentaries.

TABLE OF CONTENTS



EXECUTIVE SUMMARY

Ransomware has become a national security concern in recent years. Governments have expanded their disruptive action from infrastructure takedowns and arrests to sanctions, indictments, and public exposure. Yet, these efforts are often applied opportunistically and assessed in isolation, making it difficult to judge which interventions generate lasting impact and which deliver only short-term disruption.

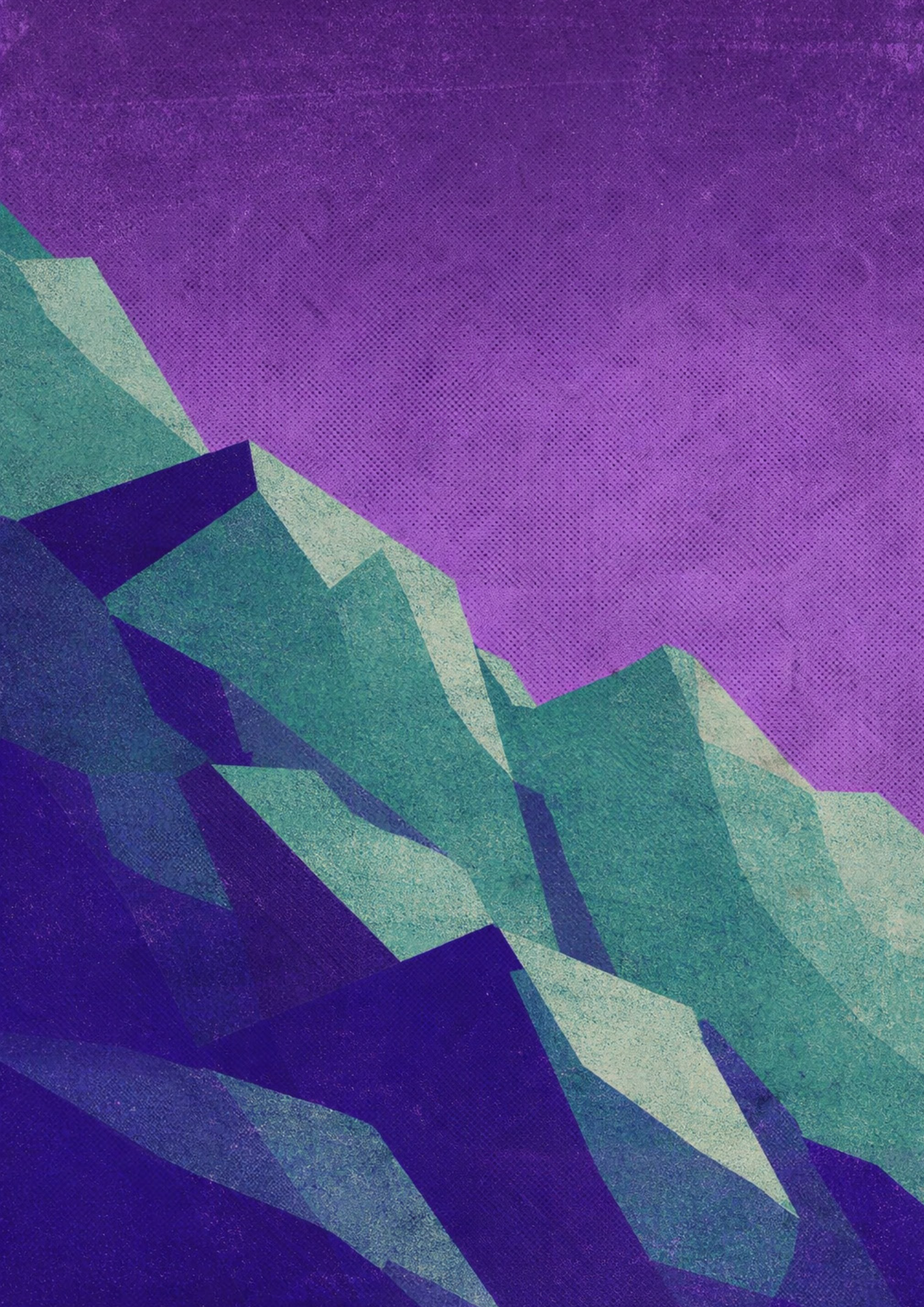
This report addresses a central analytical gap: the absence of a shared, indicator-based framework for assessing the impact of ransomware interventions and countermeasures. It introduces a practical framework that defines ransomware interventions and evaluates their impact across four dimensions: severity, scope, longevity and reversibility, and signalling value. Together, these dimensions provide a structured way to describe, assess, and compare the effects of different counter-ransomware actions without relying on headline narratives or single metrics.

The framework is designed to be usable under real-world constraints. It supports graded assessment rather than precise measurement, allows comparison across interventions that differ in scale and design, and distinguishes between actor-level effects and broader ecosystem consequences. By separating different dimensions of impact, the framework makes trade-offs visible and enables more consistent analysis across cases and over time.

To demonstrate how the framework can be applied in practice, the report uses four government-led interventions as illustrative cases: against REvil (2021-22), Operation Ladybird against Emotet (2021), against Hive (2022-23), and Operation Cronos against LockBit (2024). These cases are not treated as definitive outcome evaluations, but as structured examples of how the framework can be used to assess impact across different intervention types and targets.

Applied across these cases, the framework shows that visibility should not be conflated with effectiveness and that impact is rarely one-dimensional. Interventions can score highly on some dimensions while remaining limited or reversible on others. The framework also highlights how different intervention designs tend to emphasise different dimensions of impact, reinforcing the value of a multi-dimensional approach.

Overall, the framework offers policymakers, operational teams, and partners a common language for assessing impact, comparing interventions, and building cumulative knowledge across counter-ransomware efforts.



INTRODUCTION

Ransomware has moved from the margins of cybercrime to the centre of national security concerns. What began as isolated attacks against individuals in the 1990s and 2000s has grown into a widespread extortion ecosystem, capable of disrupting critical infrastructure and undermining public trust in government and institutions.

Governments and law enforcement agencies have stepped up efforts to counter this threat, deploying a wide range of measures, from arrests and sanctions to infrastructure takedowns and public attributions. Yet, these countermeasures are often applied opportunistically and assessed in isolation, making it difficult to judge which interventions deliver meaningful, lasting impact and which only achieve short-term disruption.

There is currently no consistent, standardised framework that allows policymakers, law enforcement officers, and private-sector researchers to systematically evaluate and compare these actions or to understand how they interact and affect the broader ransomware ecosystem. Frameworks exist which allow for the recording of counter-ransomware measures and for their assessment according to under-specified criteria. These frameworks, however, are of limited utility to policymakers and decisionmakers. This is because they fall short of providing a systematic tool for evaluation and comparison and lack an indicator-based and graded framework for assessing effectiveness of counter-ransomware interventions. Pre-existing frameworks also fall short of evaluating impact against the ransomware ecosystem opposed to the threat actor in isolation and thus fail to measure intended and unintended systemic consequences.

This gap matters because it leaves policymakers and operational teams without a reliable way to judge which efforts are most effective in disrupting ransomware. In the absence of a shared, indicator-based understanding of impact, it is difficult to design and sequence effective interventions, to justify the resources required for sustained campaigns, and to determine whether the broader counter-ransomware strategy is making the ecosystem less hospitable to criminal actors. Without a common framework, assessments tend to rely on anecdote, headline successes, or narrow operational metrics, obscuring both unintended consequences and opportunities to reinforce or coordinate interventions for greater cumulative effect.

This report addresses that gap. It sets out a practical, evidence-based framework for assessing the impact of ransomware interventions and countermeasures. The framework is designed to help governments and their partners prioritise resources, target interventions that generate the greatest systemic disruption at the lowest cost, and avoid unintended consequences that might strengthen cybercriminal groups, such as affiliate migration or market consolidation.

The analysis draws on multiple sources: open-source reporting, structured interviews with practitioners involved in ransomware operations and response, and a series of validation workshops with government officials, law enforcement representatives, and private-sector experts. These inputs ensure that the framework reflects both operational realities and the constraints faced by those designing and executing interventions.

The framework consists of two dimensions. First, we outline the landscape of ransomware interventions and countermeasures, explaining how they differ in duration, cadence, partnerships, and the parts of the ransomware ecosystem they target. Second, we define impact across four measurable dimensions – severity, scope, longevity and reversibility, and signalling value – and provide indicators to evaluate these consistently across cases. Combining these dimensions allows for structured analysis and meaningful comparison across interventions.

To demonstrate how the framework functions in practice, we apply it to four prominent counter-ransomware interventions: the operations against REvil (2021), Operation Ladybird to dismantle the Emotet botnet (2021), the takedown of Hive (2022-23), and Operation Cronos against LockBit (2024). These cases were selected because they represent distinct intervention types and targets, while all involving large-scale, government-led action with sufficient public reporting to allow systematic, open-source analysis. As such, they illustrate the minimum level of assessment possible while using the framework; a government organisation applying the same approach with access to classified and operational data would be able to produce more granular evaluations.

These cases show how the framework can be used to compare impact across different ransomware-related activities. They span interventions focused on technical infrastructure and shared services (Emotet), organisational networks and monetisation (REvil and Hive), and a combined approach targeting infrastructure, organisation, and branding simultaneously (LockBit). Applying the framework across these cases enables structured comparison across severity, scope, longevity and reversibility, and signalling value.

The application of the framework also underscores that visibility should not be conflated with effectiveness. Many counter-ransomware interventions generate sharp operational disruption and strong public signals yet struggle to produce durable change without follow-on measures or complementary actions. By separating severity, scope, longevity and reversibility, and signalling value, the framework provides a way to assess these trade-offs explicitly and to distinguish short-term disruption from more sustained ecosystem effects. This distinction is critical for designing counter-ransomware strategies that move beyond headline outcomes towards lasting impact.

EXISTING APPROACHES AND BEST PRACTICES

This section analyses existing approaches to measuring and assessing the impact of counter-ransomware interventions. The analysis shows that, despite the growing scale and visibility of counter-ransomware activity, there is no standardised, indicator-based framework in use at either the national or international level for evaluating and comparing impact across cases.

Where impact assessments do occur, they are typically shaped by generic risk or intelligence assessment frameworks rather than tools designed for ransomware specifically. A former US official stated in an interview that while all US intelligence analysts are trained in impact assessments, this training is not explicitly tailored to the cyber domain or to cybercrime.[1] The interviewee further noted that existing guidance on applying impact assessment methodologies to cyber operations – such as the Cyber Deterrence Framework – is under-used in practice. An audit of the US Department of Justice's (DOJ's) counter-ransomware strategy in 2024 also suggested that the Department's existing metrics for ransomware do not capture the effectiveness of its disruptive activities against malicious actors.[2] Similarly, in the UK, one law enforcement officer explained that the impact of cybercrime countermeasures is assessed using the Management of Risk in Law Enforcement (MoRiLE) framework, a generic and mandatory risk assessment tool used across UK law enforcement, rather than a framework designed to assess cyber effects.[2]

> "US Department of Justice's existing metrics for ransomware do not capture the effectiveness of its disruptive activities against malicious actors.

Impact assessments are often also ad hoc and organisation specific. Cyber threat intelligence experts from the German government stressed that the different agencies responsible for countering cyber threat actors assess the impact of their interventions independently and according to distinct internal approaches.[4] Furthermore, these assessments are often presented to government separately, without synthesis or a joint assessment mechanism.

[1] Authors' interview with ex-US law enforcement, November 2025.

[2] US Department of Justice, 'Audit of the Department of Justice's Strategy to Combat and Respond to Ransomware Threat and Attacks,' September 2024, https://oig.justice.gov/sites/default/files/reports/24-107.pdf.

[3] Authors' interviews with UK law enforcement, December 2025. UK officers emphasised that a specific, more granular tool tailored for ransomware would be beneficial and could aid impact or effects-led operational planning.

[4] Authors' interview with German cybersecurity officials, November 2025.

Although no dedicated impact assessment framework for ransomware interventions currently exists, pre-existing approaches do provide useful insights into how such a framework could be designed.

First, any framework must confront a basic trade-off between precision and practicality in measurement. Ideally, impact would be assessed using highly specific and quantifiable indicators, such as the number of arrests, changes in threat actor activity or online chatter, or the value of seized or frozen assets. In practice, however, such granular measurement is difficult to achieve consistently. This data is often labour intensive to collect, unevenly available across jurisdictions, and highly context-dependent, and therefore poorly suited for systematic comparison across cases or countries.

At the other end of the spectrum, many existing assessment approaches rely on broad qualitative judgements framed in terms of 'strengths' and 'weaknesses'.[5] While these approaches are easier to apply, they lack sufficient specificity and structure to enable meaningful comparison across interventions or over time.

A grade-based measurement system represents a pragmatic middle ground between these two extremes. It avoids the impracticality of fully metric-driven models while offering greater structure and comparability than purely qualitative assessments. By assigning graded judgements across clearly defined dimensions, such an approach enables systematic comparison without requiring unrealistic levels of data availability or standardisation.

There is precedent for this approach in both crime and cybercrime contexts. The UK's National Crime Agency, for example, evaluates disruptions of organised crime groups across severity and longevity dimensions, grading impacts as significant, moderate, or minor.[6] Similarly, the Defenders Disrupting Adversaries dataset from Jason Healey, Neil Jenkins, and JD Work grades 100 counter-cybercrime disruption operations by disruptive effect and disruptive duration.[7]

Second, existing research and approaches highlight a further design trade-off concerning the number of dimensions across which impact is assessed.[8] A framework that relies on a single dimension risks oversimplifying complex interventions, while one that includes too many dimensions quickly becomes unwieldy and hard to compare across cases. As such, a standardised framework should rely on a small but meaningful set of dimensions – sufficient to capture different types of impact without sacrificing usability or comparability.

---

[5] Interpol, 'A Comparative Threat Assessment on Counter Ransomware Interventions,' 20 October 2025, https://members.counter-ransomware.org/documents.

[6] National Crime Agency, 'Annual Report and Accounts 2024-2025,' 29 July 2025, https://www.gov.uk/government/publications/national-crime-agency-annual-report-and-accounts-2024-to-2025.

[7] Jason Healey, Neil Jenkins, and JD Work, 'Defenders Disrupting Adversaries: Framework, Dataset, and Case Studies of Disruptive Counter-Cyber Operations', *12th International Conference on Cyber Conflict (CyCon), 2020,* https://www.ccdcoe.org/uploads/2020/05/CyCon_2020_14_Healey_Jenkins_Work.pdf.

[8] See, for example, the OECD's evaluation criteria, which assess interventions across six dimensions: relevance, coherence, effectiveness, efficiency, impact, and sustainability. OECD. 'Evaluation Criteria,' 2025, https://www.oecd.org/en/topics/sub-issues/development-co-operation-evaluation-and-effectiveness/evaluation-criteria.html.

Third, existing approaches highlight a trade-off related to the level at which impact is assessed. Frameworks that focus exclusively on operational effects – such as disruptions to specific threat actor's activities – risk overlooking wider systemic-level consequences. At the same time, assessments that attempt to capture impact at an overly expansive level risk becoming speculative.[9]

Addressing this trade-off requires distinguishing between levels of impact. Measurement should capture not only direct effects on the targeted threat actor, but also broader effects – such as signalling or behavioural shifts among comparable actors – and ecosystem-level consequences that extend beyond any single group. This distinction matters because ransomware ecosystems rarely respond to interventions with sustained disruption; instead, they tend to shapeshift, with actors adapting, fragmenting, or displacing activity following countermeasures – leading to unintended consequences.[10] Failing to account for these dynamics risks overstating effectiveness by conflating short-term disruption with longer-term impact.

Table 1: Design trade-offs, impact assessments, and best-practice principles

DESIGN TRADE-OFF	BEST-PRACTICE PRINCIPLE
Precision vs Practicality Metrics are hard to standardise, but qualitative judgements lack structure	Use graded impact measures
Simplicity vs Comprehensiveness Too few dimensions oversimplify, but too many reduce comparability	Assess impact across a small set of meaningful dimensions
Narrow vs Broad Focus Actor-only focus misses spillovers, but system-wide focus becomes speculative	Differentiate actor and ecosystem-level effects

[9] Joyce Hakmeh and Jamie Saunders, 'The Strategic Approach to Countering Cybercrime (SACC) framework,' Chatham House, July 2024, https://www.chathamhouse.org/2024/07/strategic-approach-countering-cybercrime-sacc-framework.

[10] Interpol, 'A Comparative Threat Assessment on Counter Ransomware Interventions';; Healey, Work, and Jenkins, 'Defenders Disrupting Adversaries'; Authors' interview with German cybersecurity officials, November 2025.

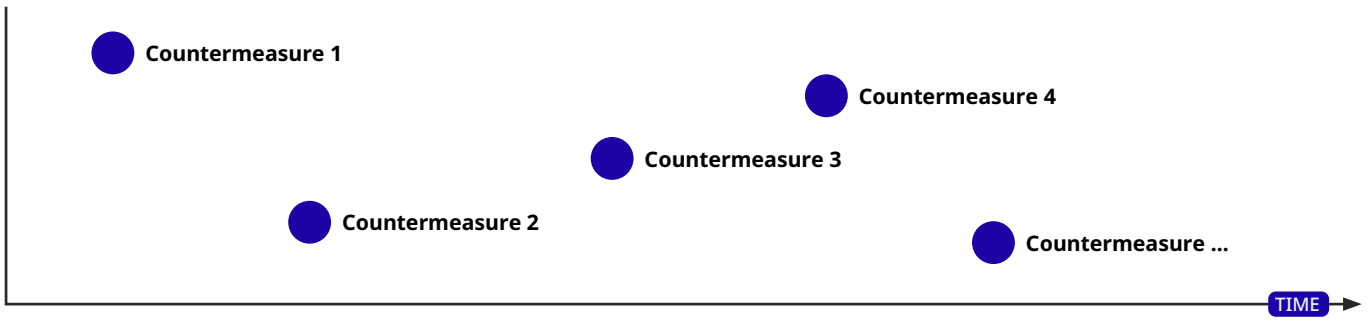
RANSOMWARE INTERVENTIONS AND COUNTERMEASURES

This report defines a ransomware intervention as an action – or a coordinated series of actions – taken by one responsible entity, or by multiple entities acting together, to influence the behaviour or operating conditions of ransomware actors.

> A ransomware intervention is an action – or a coordinated series of actions – taken by one responsible entity, or by multiple entities acting together, to influence the behaviour or operating conditions of ransomware actors.

The concept of ransomware intervention is deliberately entity-agnostic. Interventions are defined by their purpose and effects, not by the institutional identity of the actor implementing them. Law enforcement, intelligence agencies, national cybersecurity centres, regulators, private cybersecurity firms, financial institutions, and incident-response providers all undertake countermeasures that can shape ransomware activity. In this report, however, we focus on interventions where government entities are the responsible drivers. Even in these cases, the private sector is almost always involved – by providing technical access and analysis, sharing telemetry, hosting infrastructure, or supporting victim engagement. Treating interventions and countermeasures in this broader, entity-agnostic way allows us to compare very different actions on a common basis and to assess how, together, they alter both the behaviour of specific ransomware groups and the conditions of the wider ecosystem in which those groups operate.

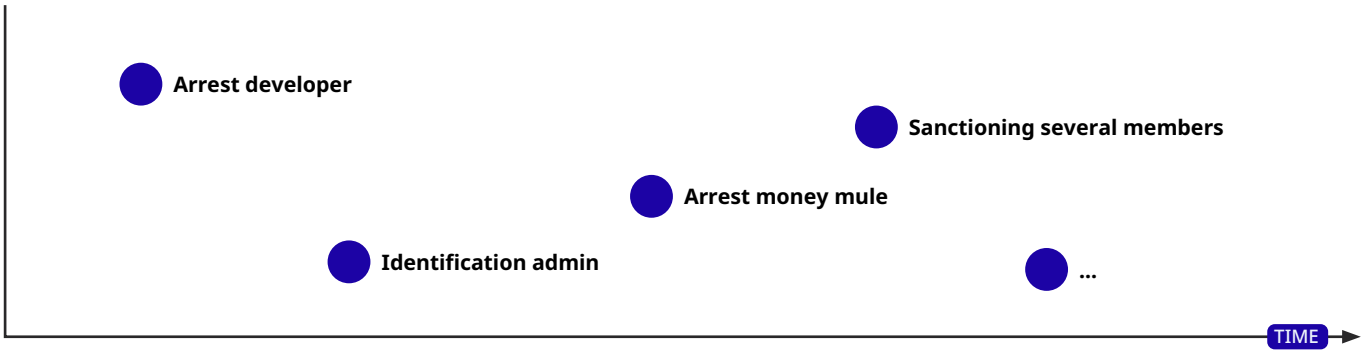
Figure 1: Conceptualization of ransomware interventions and countermeasures



Interventions are composed of countermeasures, the discrete actions that jointly produce operational, organisational, or reputational effects on a ransomware group or the wider ransomware ecosystem.

Countermeasures can vary widely. As part of a single intervention, authorities may combine the seizure of infrastructure, arrests of developers and money mules, sanctions on specific individuals, disruption of payment channels, and the freezing or confiscation of cryptocurrency assets. In some cases, the focus is clearly on one named group: law enforcement might, within a short window, seize its leak site, take over supporting servers, and detain identified members. In other cases, the same types of countermeasures are applied to shared tools and services – for example, a malware loader, a botnet, or a payment-laundering network – with the primary aim of constraining multiple ransomware operations at once. The same family of countermeasures can therefore produce actor-specific effects when tightly focused or ecosystem-wide effects when directed at common infrastructure or intermediaries.

Figure 2: Example of countermeasures part of a ransomware intervention



The scope of this report is limited to disruptive countermeasures targeting ransomware, while resilience-building countermeasures aimed at potential victims and broader society are out of scope. An indicative list of activities within scope of this report is provided below.

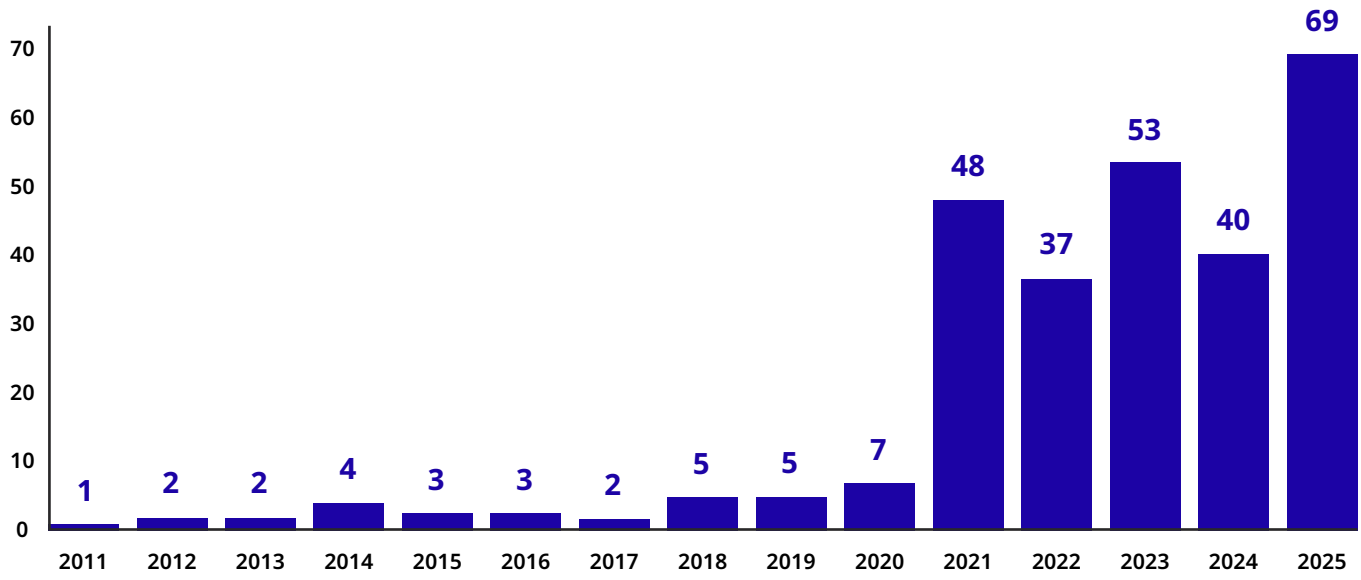
- **Technical disruption of ransomware infrastructure and tooling**, including sinkholing (botnet sinkholing redirects infected machines' traffic to controlled servers, cutting off operators' visibility and ability to issue commands), malware takeover or removal, data manipulation (eg decryption keys), and command-and-control disruption or infiltration
- **Legal takedowns and seizures of criminal infrastructure**, including botnets, domains, and servers
- **Financial disruption measures,** including sanctions, asset seizures, and payment or laundering disruptions
- **Criminal justice-focused actions against individuals**, including arrests, indictments, convictions, and extraditions

Attribution and exposure activities, including public attribution, disclosure of adversary toolsets or indicators of compromise, and official advisories

Strategic communications and media operations, including public announcements intended to signal capability, deter activity, or influence adversary behaviour

Drawing on the Virtual Routes Countermeasures Tracker, the table below shows a pronounced increase in these disruptive counter-ransomware measures over time.[11] Activity remains limited and sporadic throughout much of the 2010s, before a clear structural break around 2021, after which the number of interventions rises sharply.[12] This pattern suggests a shift from ad hoc responses to a more institutionalised and sustained counter-ransomware posture.

Figure 3: Number of ransomware countermeasures per year



How interventions differ

There are several dimensions to consider when designing ransomware interventions subsequently assessing their impact.

Duration and cadence: Some interventions are deliberately concentrated in time. These operations seek to maximise shock by synchronising as many countermeasures as possible: domains are seized, servers are reimaged or sinkholed, cryptocurrency wallets are frozen, and arrests or searches take place in multiple locations within a narrow time window.

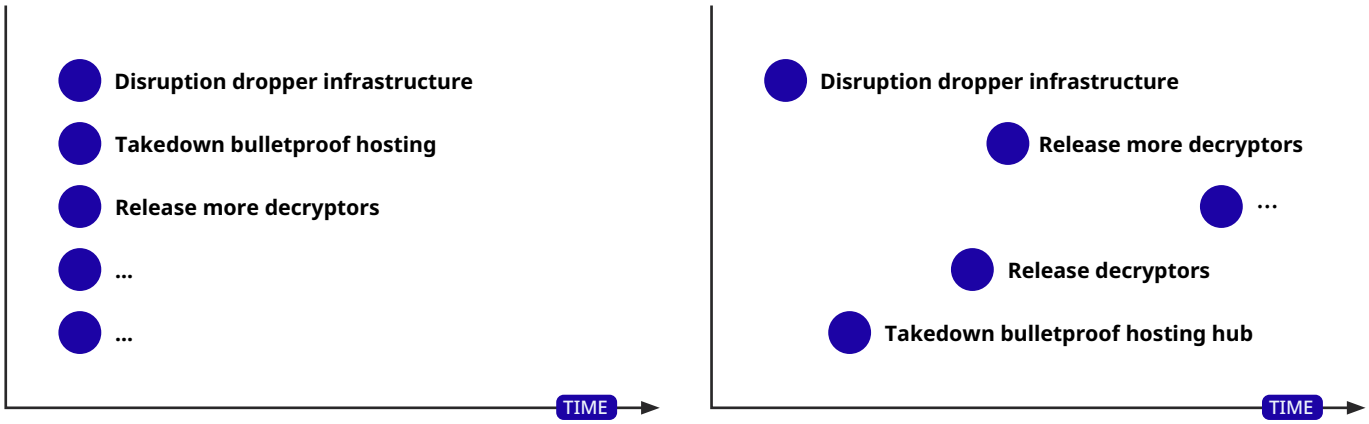
Other interventions unfold over a longer period. Authorities may spend months quietly monitoring infrastructure, inserting implants, mapping links between services, and building legal cases before

[11] Virtual Routes, 'Ransomware Countermeasures Tracker,' accessed 19 January 2026, https://virtual-routes.org/ransomware-countermeasures-tracker/.

[12] The table captures only publicly observable countermeasures. The true level of activity – particularly for covert or technical interventions – is likely higher; the increase shown here represents a conservative estimate.

moving through successive phases of disruption. Operations against large botnets or malware loaders used by multiple ransomware crews often follow this pattern: an initial infrastructure seizure might be followed by a second wave of arrests or financial actions as more actors are identified.

Figure 4: Ransomware interventions with different timing and cadence



Partnerships and responsible entities: Major ransomware interventions today rarely involve a single institution acting in isolation. They typically rely on partnerships between national law enforcement agencies, cybersecurity centres, intelligence services, financial-intelligence units, and private firms providing technical expertise or telemetry. While one agency is usually in the lead, individual countermeasures within an intervention – such as forensic exploitation of servers, execution of search warrants, cryptocurrency tracing, or victim notification – may be carried out by different partners.

That said, data from the Virtual Routes Ransomware Countermeasures Tracker shows a highly concentrated pattern of leadership in counter-ransomware activity.[13]

> Data from the Virtual Routes Ransomware Countermeasures Tracker shows a highly concentrated pattern of leadership in counter-ransomware activity.

Between 2010 and 2025, the United States was involved in over 75 percent of all recorded countermeasures. More than half of this involvement takes the form of unilateral action rather than multilateral cooperation. While coalitions do exist, they are typically anchored around US leadership, rather than reflecting broadly distributed or shared operational responsibility.[14]

[13] Virtual Routes, Ransomware Countermeasures Tracker.

Targets and targeting levels: Ransomware interventions also differ in what they are designed to target. Measures can focus on the operational level, the organisational level, or the perceptual level; many interventions combine elements across all three. Which level is prioritised shapes both how an intervention is designed and how its impact should be assessed.[15]

First, some interventions and individual countermeasures focus on how ransomware attacks are carried out, targeting different stages of the operational playbook, from gaining initial access to maintaining persistence and then on to data exfiltration, extortion, and payment collection.[16] These interventions aim to interrupt the technical and logistical steps that ransomware groups rely on to function.

In practice, these countermeasures focusing on the operational playbook take several forms. Takedowns of malware infrastructure disable servers used for command-and-control, payload hosting, data exfiltration, or affiliate management, disrupting active campaigns and forcing groups to rebuild their core systems. Authorities also target the ransomware supply chain by seizing distribution networks such as exploit kits, loaders, and distribution-as-a-service platforms, raising costs for both core groups and affiliates. In some cases, investigators or researchers obtain master keys or uncover weaknesses in ransomware code. This enables the release of decrypters, which help victims recover without paying and undermine the reputation that ransomware groups rely on to maintain credibility in the extortion economy.

[14] The percentage of operations the US is involved has slightly reduced, however.

[15] Distinction is based on Max Smeets, *Ransom War: How Cyber Crime Became a Threat to National Security* (Oxford University Press, 2025).

[16] While early ransomware campaigns typically targeted individual users in a broad, indiscriminate manner, modern groups have shifted toward larger organisations, including businesses, hospitals, and public institutions. These targets are seen as more profitable and more likely to pay substantial ransoms to restore critical operations.

Highlight box: Operation Endgame

In May 2024, a global coalition of law enforcement and judicial agencies launched Operation Endgame, an ongoing multi-phase effort to dismantle the infrastructure underpinning ransomware and related cybercrime operations.[17]

The focus was not primarily on the encryption payloads themselves, but on the 'initial access' and distribution backbone: malware droppers, loaders, botnets and command-and-control infrastructure which enable ransomware deployment. For example, the 2025 phase targeted known loader families such as DanaBot, Bumblebee, TrickBot, QakBot, and WarmCookie.

Between 19 and 22 May 2025, authorities seized or disabled approximately 300 servers, neutralised around 650 domains, and issued 20 international arrest warrants. Alongside this, approximately €3.5 million in cryptocurrency was seized in that action week, bringing the running total from the operation to about €21.2 million.[18]

The operation was coordinated across multiple continents, involving real-time collaboration between countries such as the USA, Canada, France, Germany, the Netherlands, the UK and Denmark, with private-sector partners analysing malware infrastructure and following the money. Europol executive director Catherine De Bolle described the key aim of the Operation Endgame: 'By disrupting the services criminals rely on to deploy ransomware, we are breaking the kill chain at its source.'[19]

The operation is ongoing: follow-up takedowns, intelligence-gathering, and arrests are planned; infrastructure disruption must be sustained to keep pace with evolving adversaries.

Second, other countermeasures centre on the people and logistical arrangements that enable ransomware operations and the wider ecosystem. Ransomware operations have grown beyond lone hackers to organised, networked groups that function more like traditional criminal enterprises.[20] The core team typically oversees malware development and infrastructure, while other operators carry out intrusions and deploy ransomware payloads. There are also many supporting roles within these criminal groups, such as negotiators, money

[17] Europol, 'Largest Ever Operation Against Botnets Hits Dropper Malware Ecosystem,' 30 May 2024, https://www.europol.europa.eu/media-press/newsroom/news/largest-ever-operation-against-botnets-hits-dropper-malware-ecosystem; Federal Bureau of Investigation (FBI), 'Operation Endgame: Coordinated Worldwide Law Enforcement Action Against Network of Cybercriminals,' 30 May 2024, https://www.fbi.gov/news/press-releases/operation-endgame-coordinated-worldwide-law-enforcement-action-against-network-of-cybercriminals; for later actions: Europol, 'Operation ENDGAME Strikes Again: the Ransomware Kill Chain Broken at Its Source,' 23 May 2025, https://www.europol.europa.eu/media-press/newsroom/news/operation-endgame-strikes-again-ransomware-kill-chain-broken-its-source.

[18] Ravie Lakshmanan, '300 Servers and €3.5M Seized as Europol Strikes Ransomware Networks Worldwide,' 23 May 2025, https://thehackernews.com/2025/05/300-servers-and-35m-seized-as-europol.html.

[19] *Ibid.*

[20] See Smeets, *Ransom War*.

mules, infrastructure maintainers, and individuals managing public communication channels. The rise of ransomware-as-a-service (RaaS) has enabled this expansion of personnel. Under this model, core operators lease ransomware tools to affiliates, who then conduct attacks and share ransom proceeds. This allows rapid scaling, but it also introduces internal vulnerabilities, such as uneven operational security standards and conflicts among affiliates.

Arrests, indictments, sanctions, extraditions, and the exposure of internal communications can all disrupt these human networks. When used against a specific group's core members, these actions can hollow out a particular operation. When they target cross-cutting intermediaries – such as laundering networks serving multiple groups – they can also shift trust relationships more broadly, making it harder for new partnerships to form.

Third, some measures primarily aim to influence how victims, potential affiliates, and other criminal actors perceive ransomware groups and the risks associated with them. Unlike espionage-focused state actors, ransomware groups depend on visibility to exert pressure and secure payments, making reputation and branding operationally important. Groups therefore actively manage how they are perceived. For example, after several high-profile incidents, the Snatch Team published a statement on its leak site denying it was a ransomware group at all, instead portraying itself as a data-leak collective – an effort to contest attribution and reshape its public image.[21]

Leak-site takedowns, public attributions, coordinated media messaging, and tactical disclosures about operational failures all seek to erode the perceived reliability and status of particular brands. At the group level, this can reduce victims' willingness to pay and make it harder to recruit affiliates. At the ecosystem level, repeated, visible interventions of this kind can adjust expectations more generally: they may encourage organisations to resist paying, deter some would-be affiliates, and signal that certain behaviours (for example, rebranding after a takedown) are closely monitored.

Finally, in practice, most significant ransomware interventions combine elements from all three areas. A single operation may simultaneously degrade infrastructure, detain key individuals, and deploy public messaging designed to undermine confidence in the targeted actors. Whether the resulting impact is primarily on a single group or on the wider ecosystem depends on what is targeted, how extensively shared that resource or service is, and how visible the intervention becomes to others.

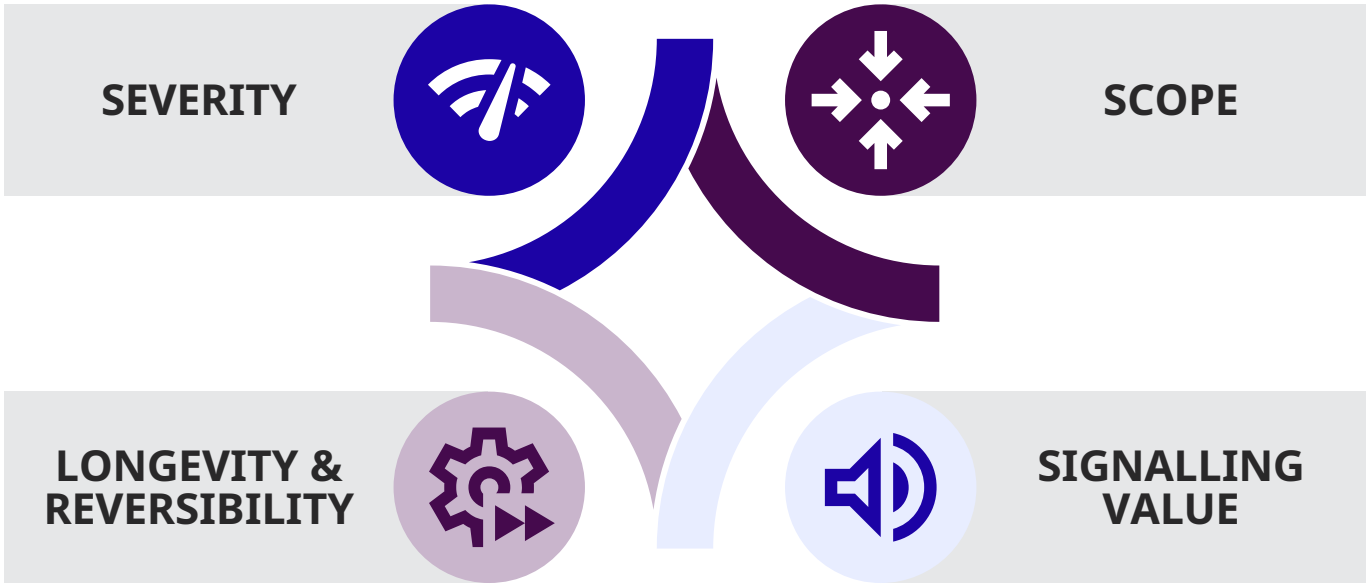
[21] Cybersecurity and Infrastructure Security Agency (CISA) and FBI, '#StopRansomware: Snatch Ransomware,' 20 September 2023, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-263a; @snatch_info (Telegram), post no. 193, accessed 19 January 2026, https://t.me/snatch_info/193; for more context on (later) Telegram posting also see: Jonathan Greig, 'Snatch Gang "Consistently Evolved" in Targeting Multiple Industries, Feds Say,' Record, 20 September 2023, https://therecord.media/snatch-ransomware-group-alert-fbi-cisa.

MEASURING IMPACT

Now that we have a clearer understanding of the interventions used against ransomware groups- and the specific countermeasures that make up those interventions, we can turn to assessing their impact. As noted earlier, although many government actions are publicly described as successes, there is rarely a shared definition of what 'impact' entails or how it should be measured across different cases. This absence of consistency makes it difficult to prioritise resources, compare interventions, or distinguish measures that generate lasting effects from those that only create short-term disruption.

Dimensions of impact

We define impact across four dimensions: severity, scope, longevity and reversibility, and signalling value. Each dimension captures a different aspect of how a countermeasure affects a ransomware group and the wider ecosystem.



Severity refers to the degree of operational damage inflicted on the targeted group. A severe intervention disrupts core activities, compromises infrastructure, or results in the arrest of key members, forcing a significant operational reset. Less severe measures may cause temporary interruptions but allow groups to resume operations easily. Severity can be observed through metrics such as downtime duration, loss of capabilities, or evidence of major internal reorganisation.

SEVERITY

DEGREE OF OPERATIONAL DAMAGE INFLICTED ON TARGETED THREAT ACTOR(S).

- Downtime duration (eg, how long group activity ceases)
- Number of core operators arrested or sanctioned
- Importance of infrastructure seized, damaged or destroyed (servers, domains)
- Confiscated crypto funds
- Evidence of major internal reorganisation or affiliate loss

Scope describes the breadth of an intervention's effects. Some actions are narrowly focused, targeting a single group or subset of actors, while others produce wider ripple effects across the ransomware ecosystem. For example, dismantling a widely used initial access broker can disrupt multiple groups simultaneously, whereas taking down a single leak site affects one operation alone. Understanding scope is essential for assessing whether a measure addresses only immediate threats or contributes to broader ecosystem-level change.[22]

SCOPE

SCOPE OF AN INTERVENTION'S EFFECTS – BOTH AGAINST THE TARGETED ACTOR AND ECOSYSTEM AS A WHOLE.

- Number of ransomware operators or affiliates affected
- Amount of infrastructure seized, damage or destroyed
- Number of supporting services (Initial Access Brokers (IABs), botnets, launderers) affected
- Geographic range of impact
- Cross-group or ecosystem-wide disruptions

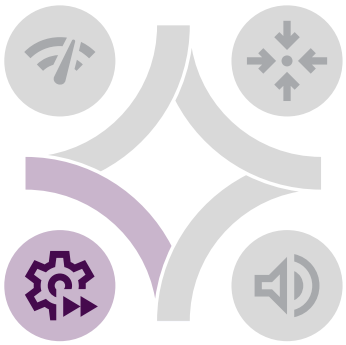
Longevity and reversibility capture how long-lasting an intervention's effects are and how easily the group can recover. Some disruptions are quickly reversible: groups can set up new infrastructure or rebrand within days or weeks. Others, such as the arrest of key developers or loss of trusted affiliates, create deeper, more enduring setbacks that are difficult to overcome. Assessing longevity helps policymakers distinguish between measures that provide short-lived relief and those that create strategic, long-term disruption.[23]

---

[22] Indicators of scope therefore extend beyond the initial target to include cross-group spillovers, geographic reach, and disruption of shared services or dependencies.

[23] Because these effects unfold over time, longevity and reversibility can only be meaningfully assessed through follow-on observation rather than immediate post-intervention outcomes.

LONGEVITY & REVERSIBILITY

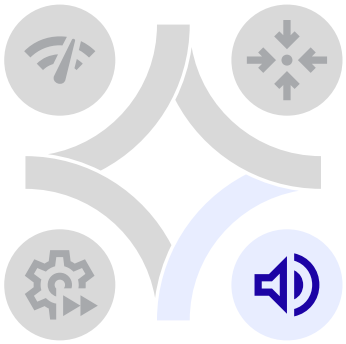


DURATION OF IMPACT AND HOW EASILY THE GROUP CAN RECOVER.

- Time until group or affiliates resume operations
- Evidence of infrastructure rebuild or rebranding
- Sustained reduction in attack volumes
- Loss of trust or recruitment setbacks

Finally, signalling value reflects the broader message sent to other ransomware groups, potential affiliates, and victims. Even an intervention with limited direct operational impact can influence behaviours and perceptions. A highly publicised takedown can deter future affiliate recruitment, reduce victim willingness to pay, and signal government resolve and capability. Signalling also shapes norms and expectations, reinforcing or undermining collective efforts to discourage ransom payments.

SIGNALLING VALUE



BROADER MESSAGE SENT TO OTHER ACTORS AND INFLUENCE ON PERCEPTIONS AND BEHAVIOUR.

- Changes in dark web chatter and affiliate discussions
- Observed decline in affiliate recruitment
- Victim negotiation behaviour (eg, increased refusal to pay)
- Media coverage and public statements from groups

Taken together, these four dimensions provide a structured way to evaluate the impact of any intervention, regardless of which countermeasures it involves or which part of the ransomware ecosystem it targets. Rather than relying on oversimplified success narratives, this approach makes it possible to compare interventions on consistent terms and to understand why certain actions generate broader or more durable effects than others. It also highlights that impact is rarely one-dimensional: an intervention may score high on severity but low on longevity, or have limited operational consequences yet significant signalling value. Assessing these dimensions side by side offers a clearer picture of how an intervention reshapes incentives, capabilities, and behaviour within the ecosystem.

This framework also helps identify where individual measures may be insufficient on their own but powerful when combined. For example, a technical takedown that is severe but easily reversible may achieve greater long-term effect when coupled with legal action, public communication, or financial disruption.

> By breaking impact into its constituent parts, policymakers can design interventions that reinforce each other rather than operate in isolation, and can prioritise combinations that deliver both immediate operational consequences and longer-term strategic benefits.

Intended framework users and assessors

The framework is designed primarily to support government agencies in thinking systematically about the impact of ransomware countermeasures. This does not imply, however, that impact assessments must be conducted by government actors only or in isolation. In practice, such assessments are frequently led or co-produced by private-sector actors, academic researchers, or non-governmental organisations with access to specialised data and analytical capabilities.

In almost all cases, a credible impact assessment requires data drawn from multiple sources: law enforcement reporting, threat intelligence feeds, victim disclosures, blockchain analysis, infrastructure telemetry, and open-source reporting. As a result, impact assessment should be understood as a collective analytical exercise, even when a single agency is formally in the lead. The framework is therefore intended to facilitate shared analysis across organisational boundaries, rather than to prescribe a single institutional owner.

Harms beyond the framework

The framework deliberately focuses on the impact of countermeasures on ransomware actors and the wider ecosystem, rather than on the full spectrum of harms caused by ransomware incidents themselves. Ransomware generates a wide range of first-, second-, and third-order harms, including psychological, social, reputational, and physical harms that extend well beyond financial loss.[24]

Some of these harms intersect indirectly with countermeasures. For example, the takedown of a ransomware group or the arrest of an individual responsible for an attack may, for some victims, help to deal with emotional trauma, restore a sense of justice, or reduce feelings of shame and self-blame. For others, the renewed public attention associated with arrests or court proceedings may reopen distressing experiences or amplify reputational harm.

---

[24] Jamie MacColl, Pia Hüsch, Gareth Mott, James Sullivan, Jason R. C. Nurse, Sarah Turner, and Nandita Pattnaik, *The Scourge of Ransomware: Victim Insights on Harms to Individuals, Organisations and Society*, RUSI Occasional Paper, January 2024 (Royal United Services Institute for Defence and Security Studies, 2024), https://static.rusi.org/ransomware-harms-op-january-2024.pdf.

These victim-centred effects are real and consequential, but they are not explicitly measured within this framework. This omission is intentional. The framework should therefore be read as complementary to harms-based analyses, not as a substitute for them. Together, the two perspectives provide a more complete picture: one focused on how interventions affect adversaries and ecosystems, and the other on how ransomware affects individuals, organisations, and society.

Impact is not effectiveness

It is important to underline that this is an impact framework, not an effectiveness or cost-benefit framework. The framework does not assess whether the resources invested in a countermeasure – in terms of funding, personnel, time, or political capital – are 'worth it' relative to alternative interventions.

As a result, the framework does not answer questions such as whether a highly resource-intensive intervention with severe impact is preferable to a lower-cost intervention with only moderate impact. Nor does it assume that high impact across all dimensions is always desirable. In some cases, policymakers may deliberately pursue limited or targeted impact – a precision intervention designed to disrupt a specific capability, gather intelligence, test access, or exploit a fleeting operational opportunity – while fully recognising that it will not meaningfully change the targeted group's long-term trajectory or the broader ecosystem.

The framework is therefore best understood as a tool for describing and comparing impact, not for adjudicating normative value or resource efficiency. Those judgments require additional policy, legal, and political considerations beyond the scope of this framework.

Timeframe and impact assessment

Finally, the timeframe over which impact is assessed matters. Short-term assessments may emphasise immediate operational disruption, while longer-term assessments are more likely to capture recovery, adaptation, rebranding, or ecosystem-level spillover effects. The same intervention can therefore appear more or less impactful depending on when it is evaluated.

That said, the structure of the framework itself does not change over time. The four impact dimensions – severity, scope, longevity and reversibility, and signalling value – remain relevant regardless of whether an assessment is conducted weeks, months, or years after an intervention. What changes is not the framework, but the empirical evidence available to populate it. Being explicit about the assessment window is therefore essential for transparency and comparability across cases.

SEVERITY

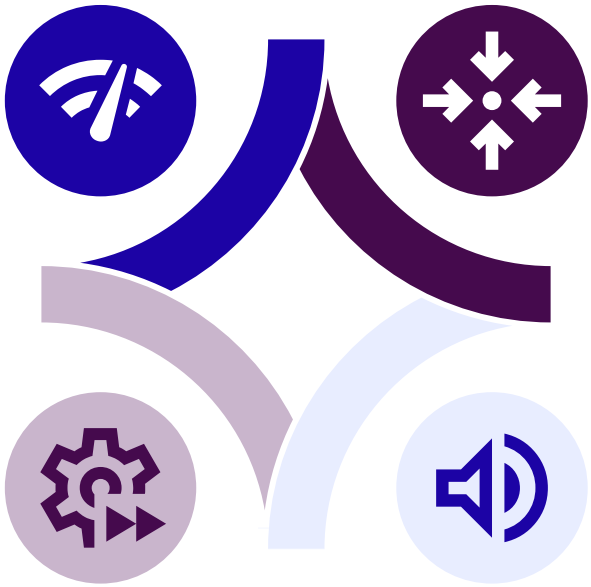
DEGREE OF OPERATIONAL DAMAGE INFLICTED ON TARGETED THREAT ACTOR(S).

- Downtime duration (eg, how long group activity ceases)
- Number of core operators arrested or sanctioned
- Importance of infrastructure seized, damaged or destroyed (servers, domains)
- Confiscated crypto funds
- Evidence of major internal reorganisation or affiliate loss

SCOPE

SCOPE OF AN INTERVENTION'S EFFECTS – BOTH AGAINST THE TARGETED ACTOR AND ECOSYSTEM AS A WHOLE.

- Number of ransomware operators or affiliates affected
- Amount of infrastructure seized, damage or destroyed
- Number of supporting services (Initial Access Brokers (IABs), botnets, launderers) affected
- Geographic range of impact
- Cross-group or ecosystem-wide disruptions



LONGEVITY & REVERSIBILITY

DURATION OF IMPACT AND HOW EASILY THE GROUP CAN RECOVER.

- Time until group or affiliates resume operations
- Evidence of infrastructure rebuild or rebranding
- Sustained reduction in attack volumes
- Loss of trust or recruitment setbacks

SIGNALLING VALUE

BROADER MESSAGE SENT TO OTHER ACTORS AND INFLUENCE ON PERCEPTIONS AND BEHAVIOUR.

- Changes in dark web chatter and affiliate discussions
- Observed decline in affiliate recruitment
- Victim negotiation behaviour (eg, increased refusal to pay)
- Media coverage and public statements from groups

CASE STUDIES

The framework becomes clearer when tested against real-world interventions. The four cases examined here – the operations against REvil (2021–22), Operation Ladybird taking down Emotet (2021), the intervention against Hive (2022–23), and Operation Cronos against LockBit (2024) – were all led by government agencies and rank among the most significant counter-ransomware actions undertaken since 2020.

These cases were deliberately selected because of their scale and visibility. By definition, this skews the sample towards more consequential interventions rather than routine or low-level actions. This focus allows the framework to be stress-tested against cases where governments deployed multiple countermeasures simultaneously and where claims about impact are most frequently made. Even within these high-profile interventions, the framework reveals substantial variation across severity, scope, longevity and reversibility, and signalling. That internal variation – where an intervention produces strong effects along some dimensions but weaker or more ambiguous effects along others – is analytically important and often obscured by headline narratives of 'success' or 'failure'.

That said, the cases are not intended as full impact assessments. The analysis is necessarily constrained, as it does not draw on classified sources and instead relies on public reporting and limited insights from those involved. What is presented here therefore reflects the minimum level of analysis possible using the framework. A government organisation applying the same approach would have access to richer classified and operational data, enabling a more granular and precise assessment of how individual countermeasures shaped both the targeted actors and the wider ransomware ecosystem.

Interventions against REvil

REvil was a prolific and very successful RaaS operation that ran until 2022 and was responsible for some of the most significant ransomware attacks to date. It first appeared in April 2019 and was initially branded as 'Sodinokibi'.[25] REvil is believed, due to technical and operational overlaps, to have been launched and run by individuals linked to GandCrab ransomware.[26]

In August 2019, REvil demonstrated its ambition with a major supply-chain attack via a managed service provider, which disrupted 23 municipalities in Texas and carried a ransomdemand of $2.5

[25] John Fokker, 'Dismantling a prolific cybercriminal empire: REvil arrests and reemergence,' Trellix, 29 September 2022, https://www.trellix.com/en-gb/blogs/research/dismantling-a-prolific-cybercriminal-empire/.

[26] CrowdStrike and other threat intelligence firms assess that the same core operators (tracked as Pinchy Spider) were behind both groups, with REvil emerging shortly after GandCrab's announced shutdown in 2019. Technically, REvil reused and refined elements of GandCrab's codebase, including similar encryption logic, execution flows, and infrastructure design, while addressing known weaknesses exposed in earlier GandCrab versions. The two groups also used comparable access vectors, such as compromised managed service provider access, and similar rules around targeting and revenue sharing. Adam M, 'The Evolution of PINCHY SPIDER from GandCrab to REvil,' CrowdStrike, 7 July 2021, https://www.crowdstrike.com/en-us/blog/the-evolution-of-revil-ransomware-and-pinchy-spider/.

million – one of the largest ransomware asks at the time. The group moved quickly to adopt double-extortion tactics, combining data theft with encryption to increase pressure on victims.[27] In early 2020, REvil further consolidated its position within the ransomware ecosystem by launching a leak site known as the 'Happy Blog'.[28]

REvil went to lengths to market its brand and was not, at least initially, afraid of public notoriety. In September 2020, the REvil operator 'Unknown' deposited 99 Bitcoin (worth $1 million at the time) on a cybercriminal forum to attract potential affiliates.[29] The following year, Unknown appeared in an interview with cybersecurity media outlet the Record, boasting that, 'For me personally, I just love doing [ransomware] and making a profit from it.'[30]

REvil's most impactful operations came in the summer of 2021. In May, REvil disrupted food supply chains after it was used to target JBS Foods, the world's largest meat processing company. JBS subsequently paid an $11 million ransom to suppress data stolen as part of the attack.[31] In July, REvil was involved in a highly publicised and damaging attack against Kaseya, a software supplier to managed IT service providers. At least 800 downstream businesses were affected by the attack, with REvil demanding a staggering $70 million for a universal decryption key.[32] Both of these incidents contributed to the emergence of ransomware as a national security issue in the US and other countries in 2021.

Targets of the intervention

Following the Kaseya incident, US President Joe Biden warned that the United States would take 'any necessary action' to defend US infrastructure and pledged 'the full resources of the government' to aid the investigation.[33] This public signalling reflected the elevation of REvil from a high-impact criminal group to a national-level priority.

---

[27] By December 2019, REvil was using double extortion to threaten the release of stolen data in the CyrusOne incident. That same month, the group also targeted Travelex, extracting a $2.3 million ransom. Lawrence Abrams, ' Another Ransomware Will Now Publish Victims' Data If Not Paid,' 12 December 2019, https://www.bleepingcomputer.com/news/security/another-ransomware-will-now-publish-victims-data-if-not-paid/; Lawrence Abrams, "Sodinokibi Ransomware Says Travelex Will Pay, One Way or Another," *BleepingComputer*, January 9, 2020, https://www.bleepingcomputer.com/news/security/sodinokibi-ransomware-says-travelex-will-pay-one-way-or-another/.

[28] The site was used to publish stolen data and later to auction material from victims who refused to pay. This approach drew wider attention in May 2020, when REvil exfiltrated 756 GB of data from the law firm GSMLaw, whose clients included Donald Trump, Madonna, and Lady Gaga, and auctioned the data after negotiations failed. Ionut Ilascu, 'REvil Ransomware Found Buyer for Trump Data, Now Targeting Madonna,' *BleepingComputer*, 18 May 2020, https://www.bleepingcomputer.com/news/security/revil-ransomware-found-buyer-for-trump-data-now-targeting-madonna/.

[29] Lawrence Abrams, 'REvil ransomware deposits $1 million in hacker recruitment drive,' *BleepingComputer*, 28 September 2020, https://www.bleepingcomputer.com/news/security/revil-ransomware-deposits-1-million-in-hacker-recruitment-drive/.

[30] Dmitry Smilyanets, 'I scrounged through the trash heaps... now I'm a millionaire:' An Interview with REvil's J Unknown,' *Record*, 16 March 2021, https://therecord.media/i-scrounged-through-the-trash-heaps-now-im-a-millionaire-an-interview-with-revils-unknown.

[31] BBC News, 'Meat Giant JBS Pays $11m in Ransom to Resolve Cyber-Attack,' 10 June 2021, https://www.bbc.co.uk/news/business-57423008.

[32] Raphael Satter, 'Hackers Demand $70 Million to Liberate Data Held by Companies Hit in Mass Cyberattack,' 5 July 2021, https://www.reuters.com/technology/hackers-demand-70-million-liberate-data-held-by-companies-hit-mass-cyberattack-2021-07-05/; Paul Ducklin, 'Kaseya Ransomware Attackers Say: "Pay $70 Million and We'll Set Everyone Free,"' 5 July 2021, https://www.sophos.com/it-it/blog/kaseya-ransomware-attackers-say-pay-70-million-and-well-set-everyone-free/.

[33] The attack retriggered discussions on ransomware between Biden and Russia's president Vladimir Putin, 'US President Joe Biden and Russian President Vladimir Putin Meet in Geneva,' 16 June 2021; Ellen Nakashima and Dalton Bennett, 'A Ransomware Gang Shut down after Cybercom Hijacked Its Site and It Discovered It Had Been Hacked,' *Washington Post*, 3 November 2021, https://www.washingtonpost.com/national-security/cyber-command-revil-ransomware/2021/11/03/528e03e6-3517-11ec-9bc4-86107e7b0ab1_story.html; Jon DiMaggio, 'A History of REvil,' Anaylst1, accessed 6 May 2024, https://analyst1.com/history-of-revil/. On how it triggered discussions: Steve Holland and Andrea Shalal, 'Biden Presses Putin to Act on Ransomware Attacks, Hints at Retaliation,' *Reuters*, 10 July 2021, sec. Technology, https://www.reuters.com/technology/biden-pressed-putin-call-act-ransomware-attacks-white-house-2021-07-09/;

Georges De Moura and Tal Goldstein, 'What the Biden-Putin Summit Reveals about Future of Cyber Attacks - and How to Increase Cybersecurity,' World Economic Forum, 17 June 2021, https://www.weforum.org/agenda/2021/06/joe-biden-vladimir-putin-summit-cybersecurity/.

In 2021 and 2022, a series of interventions by national and international law enforcement agencies sought to dismantle REvil as a viable RaaS entity. These interventions included the compromise and takedown of REvil's infrastructure by US authorities (including US Cyber Command), a joint international investigation (Operation GoldDust) involving 17 countries that led to the arrest of multiple REvil affiliates, and the seizure of cryptocurrency.[34] The efforts to counter REvil also involved a rare intervention by Russian law enforcement against a ransomware threat actor – several individuals linked to REvil were arrested in January 2022.[35]

Several interventions directly targeted REvil's operational playbook, particularly its reliance on centralised infrastructure and trusted internal access. The centrepiece of these efforts was a US-led operation conducted during the July 2021 Kaseya incident. During the attack, US authorities gained access to REvil's infrastructure and obtained private cryptographic keys to the group's servers. At the time, this access was not disclosed publicly, in part to avoid alerting REvil's operators to the compromise.

In the immediate aftermath of the Kaseya attack, on 13 July 2021, REvil abruptly ceased operations, shutting down its infrastructure, including theHappy Blog, and leaving many victims without a channel for negotiation or recovery. Nearly three weeks later, Kaseya announced that it had received a universal decryption key from a 'trusted third party'.[36] It later emerged that the FBI had obtained the key during the initial compromise of REvil's infrastructure. The delayed release of the key drew criticism, but authorities justified the decision as part of a broader strategy aimed at preserving operational advantage while monitoring REvil's internal response.[37]

REvil was not permanently disabled at this stage. In September 2021, roughly two months after its disappearance, the group's infrastructure and leak site briefly reappeared and new victim data was posted, indicating an attempted operational revival under the same name.[38] However, this resurgence was short lived. On 17 October 2021, a core developer using the handle '0_neday' publicly acknowledged unusual traffic redirection affecting REvil's Tor infrastructure, signalling that the group's servers had once again been compromised and they were shutting down their operations again.[39] On a criminal forum, 0_neday announced that the server had been compromised and that

---

[34] On arrests, participating countries and international organisations: Australia, Belgium, Canada, Eurojust, Europol France, Germany, Interpol, the Netherlands, Luxembourg, Norway, Philippines, Poland, Romania, South Korea, Sweden, Switzerland, Kuwait, the United Kingdom, the United States. US Department of Justice, 'Ukrainian Arrested and Charged with Ransomware Attack on Kaseya Office of Public Affairs,' 8 November 2021, https://www.justice.gov/archives/opa/pr/ukrainian-arrested-and-charged-ransomware-attack-kaseya.

[35] *BBC*, 'REvil ransomware gang arrested in Russia,' 14 January 2022, https://www.bbc.co.uk/news/technology-59998925.

[36] DiMaggio, 'A History of REvil.'

[37] Ellen Nakashima and Rachel Lerman, 'FBI Held Back Ransomware Decryption Key from Businesses to Run Operation Targeting Hackers,' *Washington Post*, 21 September 2021, https://www.washingtonpost.com/national-security/ransomware-fbi-revil-decryption-key/2021/09/21/4a9417d0-f15f-11eb-a452-4da5fe48582d_story.html; Jonathan Greig, 'FBI Decision to Withhold Kaseya Ransomware Decryption Keys Stirs Debate,' *ZDNET*, 24 September 2021, https://www.zdnet.com/article/fbi-decision-to-withhold-kaseya-ransomware-decryption-keys-stirs-debate/.

[38] As UNKN had left, a new spokesperson, known simply as REvil, assumed responsibility for public communications. Lawrence Abrams, 'REvil Ransomware's Servers Mysteriously Come Back Online,' *BleepingComputer*, 7 September 2021, https://www.bleepingcomputer.com/news/security/revil-ransomwares-servers-mysteriously-come-back-online/.

[39] Lawrence Abrams, 'REvil Ransomware Shuts down Again after Tor Sites Were Hijacked,' *BleepingComputer*, 17 October 2021, https://www.bleepingcomputer.com/news/security/revil-ransomware-shuts-down-again-after-tor-sites-were-hijacked/.

authorities were actively searching for him, marking the effective end of the group.[40] It was later revealed that the US Cyber Command was responsible for the hack.[41]

Other interventions focused on weakening REvil's ability to monetise attacks and sustain affiliate participation.

> The controlled release of decryption capabilities – first through the provision of a universal key to Kaseya and later via a decrypter developed by Bitdefender and distributed through the No More Ransom initiative – directly undermined REvil's extortion leverage.

These actions reduced the expected payoff of ongoing and future attacks and signalled that payments could no longer be assumed to guarantee exclusive access to decryption.

Authorities also moved against the financial layer of the operation. In November 2021, the US Department of Justice unsealed an indictment revealing the seizure of approximately $6.1 million in Bitcoin from Yevgeniy Polyanin, a REvil affiliate. While this action targeted an affiliated individual rather than the group's core operators, it demonstrated growing law enforcement visibility into affiliate activity and ransom laundering pathways.

In parallel, law enforcement operations targeted the wider criminal network that had supported REvil and its predecessor, GandCrab. In 2021, seven affiliates were arrested in South Korea, Kuwait, Romania, and Poland. Among them was Yaroslav Vasinskyi, a key participant in the Kaseya attack, who was extradited to the United States and later sentenced to nearly 14 years in prison in May 2024. While this action targeted an individual rather than the group's core operators, it demonstrated growing law enforcement visibility into affiliate activity and ransom laundering pathways. Around the same time, the US State Department placed REvil on its rewards programme, offering up to $10 million for information identifying the group's leaders and up to $5 million for information leading to the arrest of its affiliates.[42]

---

[40] 0_neday posted on a criminal forum that, 'the server was compromised, and they were looking for me... Good luck everyone, I'm off.'

[41] Nakashima and Bennett, 'A Ransomware Gang Shut down after Cybercom Hijacked Its Site and It Discovered It Had Been Hacked.'

[42] Ellen Nakashima and Dalton Bennett, 'Ring of Ransomware Hackers Targeted by Authorities in United States and Europe,' *Washington Post*, 11 November 2021, https://www.washingtonpost.com/national-security/revil-ransomware-arrests-doj/2021/11/08/9432dfc2-409f-11ec-a88e-2aa4632af69b_story.html.

The final phase of interventions came in January 2022, when Russian authorities announced the arrest of fourteen individuals linked to REvil.[43] They also seized substantial financial assets, including cryptocurrency, cash, luxury vehicles, and computer equipment.[44] The Federal Security Service (FSB) stated that, 'the basis for the search activities was the appeal of the competent US authorities, who reported on the leader of the criminal community and his involvement in encroachments on the information resources of foreign high-tech companies by introducing malicious software, encrypting information and extorting money for its decryption.'[45] While many observers expressed scepticism about the arrests – particularly given that charges focused on illegal payment circulation rather than malware development – the action nonetheless marked a rare instance of Russian law enforcement acting publicly against a major ransomware group.

Impact analysis

Severity: The severity of the various interventions against REvil in 2021 and 2022 was very high. The takedown of REvil's infrastructure in 2021 inflicted lasting damage on the group's operational activities. Crucially, because US authorities compromised the backups of REvil's infrastructure in the summer of 2021, they were able to maintain access and deliver a second blow in October. The second takedown effectively ended REvil as a viable RaaS brand.[46]

Scope: The interventions against REvil only had a medium impact in terms of their scope. As highlighted, seven affiliates of REvil and GandCrab across four different countries were arrested. In November 2021, Europol assessed that these affiliates were linked to ransomware operations against about 7,000 victims in total.[47] One of these affiliates, Yaroslav Yasinskyi, is also believed to have been linked to the ransomware attack against Kaseya.[48] However, as noted above, no core administrators or operators were taken off the board.

In terms of the broader impact, the interventions against REvil effectively removed what was at the time the most widely used RaaS strain. Reporting by Coveware, a specialist ransomware incident response firm, highlights that in Q1 and Q2 of 2021 REvil had the largest market share of any ransomware strain (14.2% and 16.5%).[49] However, by Q4 2021 REvil had dropped out of the top ten most used variants. Unfortunately, this did little to limit the overall growth and viability of the ransomware ecosystem during this period.

---

[43] These arrests came on the same day the US government accused Russia of dispatching saboteurs to Ukraine in order to establish grounds for invasion and of having hackers cause the shutdown of numerous Ukrainian government websites. Ivan Nechepurenko, 'Russia Says It Shut Down Notorious Hacker Group at US Request,' *New York Times*, 14 January 2022, sec. World, https://www.nytimes.com/2022/01/14/world/europe/revil-ransomware-russia-arrests.html.

[44] Seized assets included over 426 million rubles, cryptocurrencies, roughly $600,000 and €500,000 in cash, computer equipment, crypto wallets, and twenty luxury cars. FSB 'Illegal Activities of Members of the Organized Criminal Community Were Suppressed,' 14 January 2022, http://www.fsb.ru/fsb/press/message/single.htm%21id%3D10439388%40fsbMessage.html.

[45] FSB, 'Illegal Activities of Members of the Organized Criminal Community Were Suppressed, 14 January 2022, http://www.fsb.ru/fsb/press/message/single.htm%21id%3D10439388%40fsbMessage.html.

[46] Although no core operators were arrested, open-source reporting has not subsequently linked REvil's core administrators or operators to other successful RaaS operations.

[47] Some of these attacks may have been against individuals rather than organisations.

[48] Ionut Illascu, 'US seizes $6 million from REvil ransomware, arrest Kaseya hacker,' *BleepingComputer*, 8 November 2021, https://www.bleepingcomputer.com/news/security/us-seizes-6-million-from-revil-ransomware-arrest-kaseya-hacker/.

[49] Coveware, 'Quarterly Reports,' https://www.coveware.com/ransomware-quarterly-reports.

Longevity and reversibility: The interventions against REvil ended it as a viable RaaS brand, and thus had a very high impact in terms of longevity and reversibility. As noted above, the compromise of REvil's backups made it challenging for administrators to restart and then maintain operations. This also meant that they could never be fully sure that US law enforcement and intelligence still had access to their infrastructure. The uncertainty and fear that their infrastructure had been compromised or that they might be unmasked and subsequently pursued by authorities, appears to have contributed to REvil's administrators' decision to suspend and then end their operations.[50] Crucially, the compromise of REvil also played on other doubts about REvil's reliability.

Signalling Value: The interventions against REvil also had a high impact in terms of their signalling value. First, they damaged REvil's standing within the ransomware ecosystem itself. Following the first takedown of REvil in July 2021, the administrators of two popular cybercriminal forums banned the account REvil used to recruit and communicate with affiliates and other actors in the ecosystem. When REvil tried to relaunch in September 2021, one cyber threat intelligence vendor observed that, 'the most common reaction was prejudice against working with REvil again'.[51] Further reputational damage followed revelations by researchers at AdvIntel, a cybersecurity company, that REvil had embedded a backdoor allowing it to divert ransom negotiations and cheat affiliates out of proceeds. At least one affiliate publicly complained about the group's trustworthiness on criminal forums, reinforcing doubts about REvil as a reliable RaaS partner.[52]

Second, the interventions signalled the growing resolve and capability of a coalition of countries to disrupt high-impact RaaS operations. In total, 17 countries participated in actions against REvil, employing a wide range of countermeasures, including offensive cyber operations, asset seizures, sanctions, and arrests. A former FBI official later argued that the operation against REvil served as a proof of concept for a more coordinated and proactive counter-ransomware approach, shaping subsequent US thinking on how such groups could be disrupted.[53]

At the same time, the signalling effects of the January 2022 arrests by Russian authorities were more ambiguous. Many experts expressed scepticism regarding their scope and intent, noting that authorities did not clarify whether any senior REvil operators were detained and that charges focused on illegal payment circulation rather than malware development.[54] Some analysts suggested that those arrested were lower-level money mules rather than core developers or administrators, while others speculated that the action may have served domestic or strategic purposes unrelated to dismantling the group's leadership.[55]

---

[50] Dimitri Alperovitch, 'REvil is down – for now,' *Lawfare*, 16 November 2021, https://www.lawfaremedia.org/article/revil-down-now.

[51] Victoria Kivilevich, 'Will the REvil Story Finally Be Over?' 25 October 2021, https://www.kelacyber.com/blog/will-the-revil-story-finally-be-over/.

[52] DiMaggio, 'A History of REvil.'

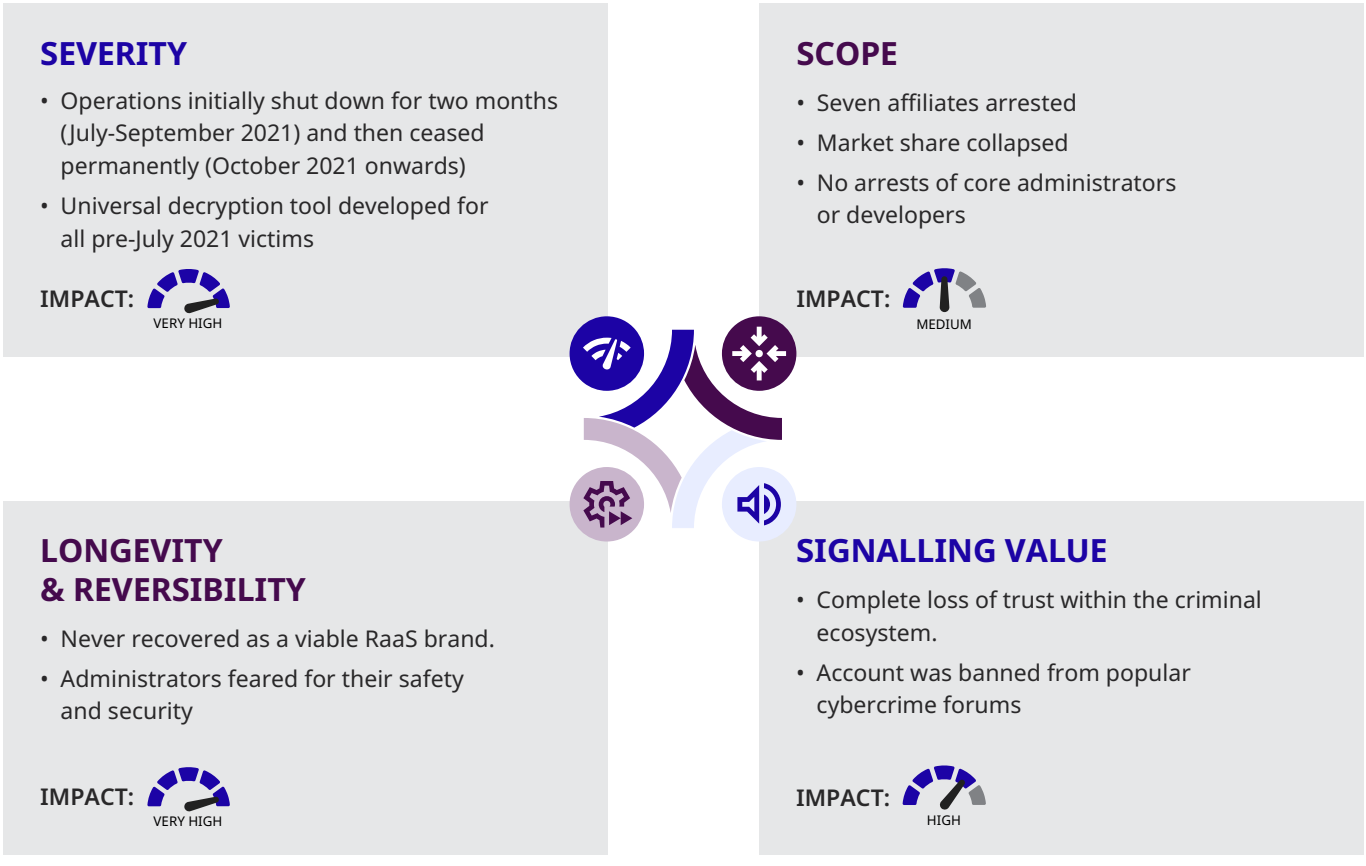
[53] Authors' interview with former FBI official, 25 November 2025.

[54] The authorities did not disclose how many individuals had been arrested, nor did they confirm whether any senior figures were among them. Those detained were charged under Article 187, Part 2, of the Russian Criminal Code, concerning the 'illegal circulation of means of payment'.

[55] *BBC*, 'REvil Ransomware Gang Arrested in Russia.'

Despite this scepticism, the arrests nevertheless generated notable signalling effects within the criminal ecosystem. The collapse of REvil created space for rival groups – most notably Conti – to absorb affiliates and expand operations, while simultaneously fuelling anxiety across Russian-language cybercriminal forums about the reliability of Russia as a safe operating environment.[56] Forum discussions reflected growing fears of law enforcement infiltration, collaboration between Western agencies and Russian authorities, and the exposure of facilitators and intermediaries. An analyst described the situation as 'a major civil war' within the Russian cybercriminal underground, illustrated by public accusations that key forum operators were cooperating with law enforcement.[57] In this sense, even contested or partial enforcement actions contributed to a broader erosion of trust and stability within the ransomware ecosystem, reinforcing uncertainty about state tolerance, protection, and the long-term viability of large RaaS operations. When coupled with increased diplomatic activity against Russia in the latter half of 2021, these interventions arguably represented the high point of efforts to counter ransomware.[58]

Figure 5: Impact Assessment Interventions against REvil



[56] Also see Smeets, *Ransom War*.

[57] Arielle Waldman, 'Distrust, Feuds Building among Ransomware Groups,' TechTarget: Security, 3 February 2022, https://www.techtarget.com/searchsecurity/news/252512902/Distrust-feuds-building-among-ransomware-groups.

[58] Authors' interview with former FBI official, 25 November 2025.

Interventions against Emotet (Operation LadyBird)

Emotet was an advanced malware botnet and loader that emerged in 2014 and evolved from a banking trojan into a 'Swiss Army knife' cybercrime service.[59] By 2018-2020 it had become one of the most prevalent cyber threats worldwide, acting as what Europol would later refer to as a 'primary door opener' for other malware on a global scale.[60] Emotet's infrastructure infected millions of computers (over 1.6 million between 2020-2021 alone) and caused hundreds of millions of dollars in damage.[61] This made Emotet an essential initial access broker in the ransomware ecosystem – for example, enabling deployment of banking trojans like TrickBot or ransomware payloads such as Ryuk on infected networks.[62]

Emotet was organised as a botnet with a tiered structure. It maintained multiple command-and-control server clusters to control infected machines, making it hard to take down.[63] The malware was notorious for its polymorphic capabilities. The group frequently updated its code and modules to evade detection, even adding features like a Wi-Fi spreader to find new victims.[64]

Emotet primarily spread via large-scale spam campaigns that often hijacked email threads and impersonated trusted senders to trick users into opening malware-laced documents.[65] Once active on a victim computer, Emotet would quietly persist and download additional payloads (remote access trojans, credential stealers, or ransomware) on behalf of its cybercrime clients.[66]

In late January 2021, an international law enforcement operation dismantled the Emotet botnet. Agencies from eight countries (the Netherlands, Germany, the United States, the United Kingdom, France, Lithuania, Canada, and Ukraine) coordinated through Europol and Eurojust to simultaneously take down Emotet's global infrastructure.[67] This joint effort, code-named Operation Ladybird, was the result of nearly two years of intelligence work mapping out Emotet's servers and operators. In total, at least 700 servers worldwide used by Emotet were taken offline or confiscated.

Law enforcement 'compromised [Emotet] from the inside' rather than just shutting down servers.[68] Investigators gained access to Emotet's core command-and-control servers and pushed a fake

---

[59] Ravie Lakshmanan, 'European Authorities Disrupt Emotet — World's Most Dangerous Malware,' 28 January 2021, https://thehackernews.com/2021/01/european-authorities-disrupt-emotet.html.

[60] Europol, 'World's Most Dangerous Malware EMOTET Disrupted Through Global Action,' 27 January 2021, https://www.europol.europa.eu/media-press/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action.

[61] DOJ, 'Emotet Botnet Disrupted in International Cyber Operation,' 28 January 2021, https://www.justice.gov/opa/pr/emotet-botnet-disrupted-international-cyber-operation.

[62] On relationship between Emotet, Trickbot, and Ryuk also see: Smeets, *Ransom War*.

[63] These clusters are sometimes referred to as separate botnets or epochs.

[64] James Quinn, 'Emotet Evolves with New Wi-Fi Spreader,' Binary Defense, accessed January 19, 2026, https://binarydefense.com/resources/blog/emotet-evolves-with-new-wi-fi-spreader/.

[65] DOJ, 'Emotet Botnet Disrupted in International Cyber Operation.'

[66] *Ibid.*

[67] Europol, 'World's Most Dangerous Malware EMOTET Disrupted Through Global Action'.

[68] Malwarebytes Labs, 'Pow! Emotet's Down. Is It Out?' 27 January 2021, https://www.malwarebytes.com/blog/news/2021/01/emotets-down-is-it-out.

Emotet update to infected machines. During the botnet's regular update check, the Emotet-infected computers downloaded a law enforcement file that untethered them from the criminal controllers.[69] This special payload disabled Emotet's ability to communicate with its servers, thereby preventing the installation of any further malware on victim machines. Notably, Dutch authorities also deployed a module to infected hosts that would automatically quarantine and remove Emotet in April 2021, ensuring a mass cleanup of remaining infections.[70] This coordinated takedown – simultaneously neutralising Emotet's three botnet clusters and using its own update mechanism against it – was a novel approach.

Targets of the intervention

The Emotet takedown primarily targeted the group's operational capacity.[71] By seizing hundreds of Emotet servers and cutting off its command-and-control channels, the operation dismantled Emotet's core distribution mechanism and toolkit. This directly disrupted how Emotet spread malware (spam campaigns, payload delivery) and severed the botnet's control over already-infected machines. In effect, the malware's operational backbone was broken, rendering its tactics and routines (from spam dissemination to payload dropping) immediately ineffective.

The takedown also struck at Emotet's human and logistical network. At least two arrests were made in Ukraine of individuals accused of maintaining the Emotet infrastructure, who face up to twelve years in prison.[72] In addition, investigators identified other co-conspirators and even some of Emotet's criminal customers through financial records and login data.

Impact analysis

Severity: The severity of the January 2021 Emotet takedown was very high. In one coordinated action, law enforcement delivered a major blow to Emotet's operations: the botnet's entire command infrastructure was captured or neutralised, and it ceased functioning overnight. Security researchers noted that the takedown 'wiped out [Emotet's] infrastructure and prevent[ed] further infections'.[73] By disconnecting over a million victim computers from the Emotet network, the operation immediately halted active malware distribution and the botnet's ability to install ransomware or other payloads on new victims. The severity was amplified by the effort to remediate victim machines via the April 2021 auto-uninstaller.

---

[69] DOJ, 'Emotet Botnet Disrupted.'

[70] Catalin Cimpanu, 'Authorities Plan to Mass-Uninstall Emotet From Infected Hosts on April 25, 2021,' ZDNet, 27 January 2021, https://www.zdnet.com/article/authorities-plan-to-mass-uninstall-emotet-from-infected-hosts-on-april-25-2021/.

[71] Unlike a ransomware gang, Emotet did not cultivate a public-facing brand to threaten victims, but it did have a reputation in underground circles as a reliable service provider.

[72] Ravie Lakshmanan, 'European Authorities Disrupt Emotet — World's Most Dangerous Malware'.

[73] Selena Larson, Daniel Blackford, and Garrett G, 'The First Step: Initial Access Leads to Ransomware,' Proofpoint, 16 June 2021, https://www.proofpoint.com/us/blog/threat-insight/first-step-initial-access-leads-ransomware.

Scope: By nature of the Emotet's purpose as a malware botnet, Emotet takedown's impact went far beyond just the Emotet group. As said, Emotet had been a critical pipeline for many ransomware gangs, so its removal had a broad disruptive effect on multiple malware campaigns. According to Nigel Leary, then deputy director of the UK National Crime Agency (NCA), 'Emotet was instrumental in some of the worst cyber attacks in recent times' and enabled up to seventy percent of the world's malwares, including the likes of Trickbot and Ryuk, which have had significant economic impact on UK businesses.[74]

Longevity and reversibility: The takedown had a medium impact against Emotet in terms of longevity and reversibility. While the takedown kept Emotet offline for a substantial period, this effect was not permanent. For roughly ten months – from late January 2021 until November 2021 – Emotet's operators were unable to reconstitute the botnet or resume large-scale activity.[75] In the fast-moving cybercriminal ecosystem, this represents a significant interruption and points to a moderate level of impact longevity. Law enforcement's multi-faceted approach (taking down servers, cleaning infections, arresting operators) made it difficult to simply restart the botnet in the short term. Indeed, Emotet's absence throughout two-thirds of 2021 suggests that the countermeasures imposed a serious logistical and technical hurdle to revival.

However, the visible decline in malspam – large-scale malicious email campaigns used to distribute malware – did not last as long as Emotet's absence. According to Proofpoint, an email security service company, other malware families that perform similar loader functions – like Trickbot, Dridex, Qbot, IcedID, ZLoader, and Ursnif - did start to fill the gap quickly, continuing to provide access for ransomware operators.[76] In other words, the botnet ecosystem rebalanced quickly with Emotet access to attackers.

> When Emotet did resurface within the ecosystem, the group showed signs of operational learning and adaptation from the takedown.

Research from ESET, a cybersecurity company, noted that post-takedown, Emotet's developers put a lot of effort into improving modules and obfuscation to evade tracking, and they experimented with new infection vectors, like malicious Windows shortcuts and Excel add-ins, once Microsoft disabled the VBA macro method they previously relied on.[77] However, this adaptability had limits: Emotet's

[74] Alexander Martin, 'Emotet: Police Raids Take Down Botnet That Hacked 'Millions of Computers Worldwide,'" *Sky News*, 27 January 2021, https://news.sky.com/story/emotet-police-raids-take-down-botnet-that-hacked-millions-of-computers-worldwide-12200460.

[75] ESET Research, 'ESET Research Follows the Comeback of the Infamous Botnet Emotet, Targeting Mainly Japan and South Europe,' 6 July 2023, https://www.eset.com/us/about/newsroom/press-releases/eset-research-follows-the-comeback-of-the-infamous-botnet-emotet/.

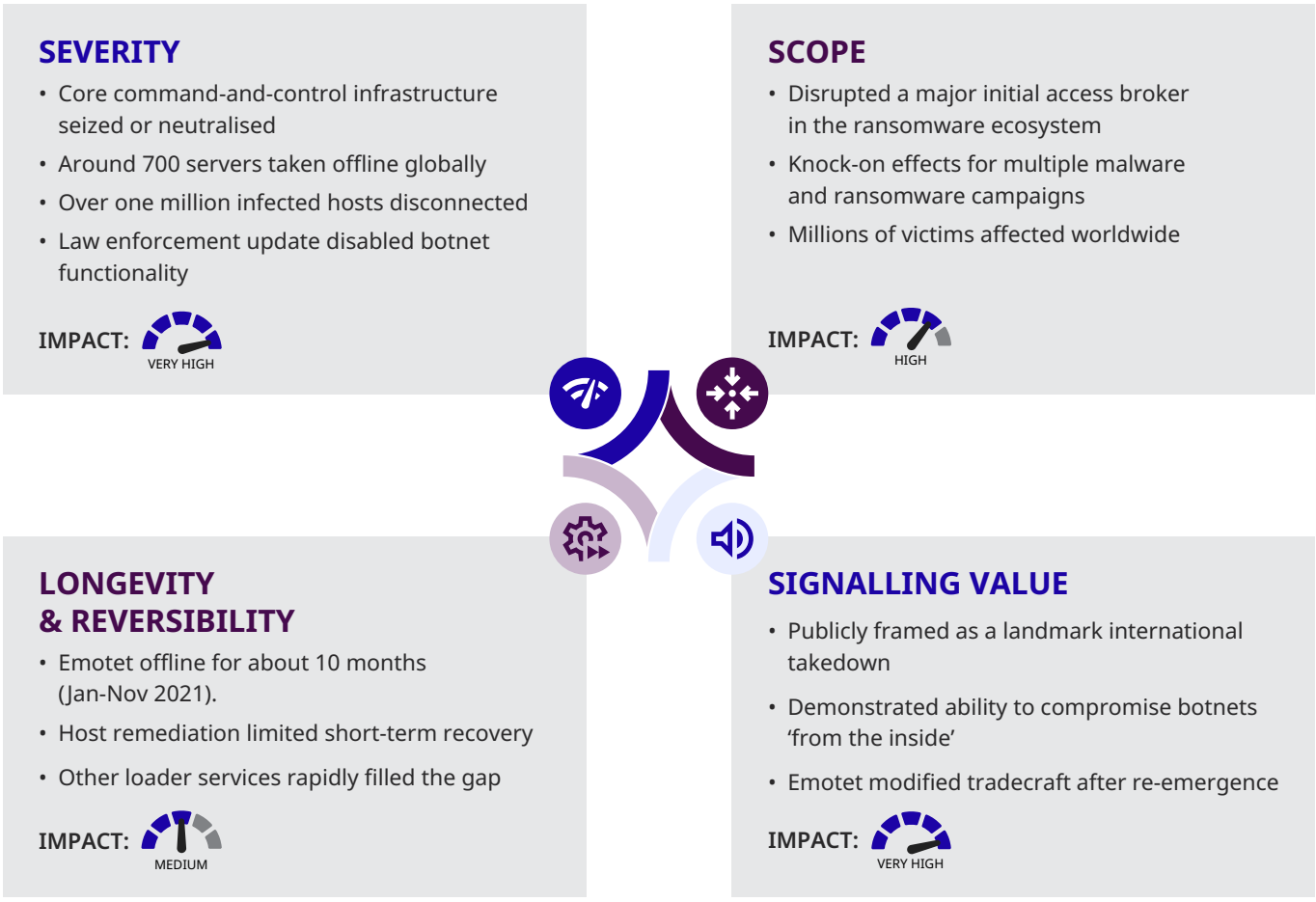
[76] Larson, Blackford, and G, 'The First Step: Initial Access Leads to Ransomware.'

operators struggled to find an attack technique as effective as their old macro-based approach, and their campaign volumes in 2022-23 remained below former levels. By April 2023, Emotet activity had dwindled again, suggesting persistent challenges or another shutdown.

Signalling Value: The takedown of Emotet was a publicly celebrated victory against cybercrime. Europol and other agencies issued press releases boasting that one of the most notorious malware threats of the decade had been knocked offline. Media coverage was global and prominent, often referring to Emotet as 'the world's most dangerous malware'. The director of the FBI explicitly stated that the operation 'is an example of how much we can achieve when we work with international partners to combat the cyber threat. … [we are] committed to imposing risk and consequences on cybercriminals.'[78]

It is unclear whether the arrests and the identification of some Emotet customers actually impacted the assuredness of criminals who previously felt untouchable. Perhaps the change the implementation of new evasion techniques, as previously discussed, is an indication that the takedown did influence the confidence of the Emotet group members.[79]

Figure 6: Impact Assessment Interventions Against Emotet



[77] ESET Research, 'ESET Research Follows the Comeback of the Infamous Botnet Emotet.'

[78] DOJ, 'Emotet Botnet Disrupted.'

Interventions against Hive

Hive ransomware was a prolific but relatively short-lived RaaS brand that first emerged in June 2021.[80] The group behind it employed double extortion tactics and ran a data leak site, 'HiveLeaks'. In 2022, following the collapse of Conti, Hive became one of the most popular RaaS brands in the ransomware ecosystem.[81] By the end of the year, Hive had been used to compromise more than 1,500 victims and had generated at least $100 million ransom payments.[82] Some individual ransom payments paid to Hive reportedly ran into the tens of millions of dollars.[83]

Like REvil, Hive's success brought the attention of law enforcement. In July 2022, FBI cyber operators gained access to Hive's network. Instead of immediately disrupting Hive's infrastructure, the FBI instead used this access to covertly generate and distribute decryption keys for hundreds of Hive victims.[84] The FBI remained undetected on Hive's network for six months and in some cases even pre-empted attacks. According to then FBI director Christopher Wray, in one case they used their access and visibility into Hive's operations to identify the final stages of an attack against a university, which allowed them to notify the university before the ransomware could be deployed.[85]

The operation against Hive ended in January 2023 when the FBI and Dutch and German police used courts to seize Hive's infrastructure, including two servers in Los Angeles that Hive used for storing data.[86] After the takedown, Hive ceased operating, although its administrators are believed by some analysts to have started a new RaaS operation, Hunters International.[87]

Targets of the intervention

The operation primarily targeted Hive's ability to monetise its operations. As then US Deputy Attorney General Lisa Monaco put it, 'we turned the tables on Hive and busted their business model.'[88] By generating and distributing decryption keys, US authorities and international counterparts aimed

---

[79] The takedown also encouraged closer cooperation between law enforcement and industry (eg. sharing botnet data with internet service providers, computer emergency response teams, and security vendors like Spamhaus) to prevent future abuse. Spamhaus, 'Emotet Infrastructure Disrupted After Coordinated Action,' 29 January 2021, https://www.spamhaus.org/resource-hub/malware/emotet-infrastructure-disrupted-after-coordinated-action/.

[80] FBI, IC3 Alert: Indicators of Compromise Associated with Hive Ransomware (TLP:WHITE), 25 August 2021, https://www.ic3.gov/CSA/2021/210825.pdf

[81] Some Conti teams likely became affiliates of Hive, according to AdvIntel and Chainalysis. See: Sergiu Gatlan, 'Costa Rica's public health agency hit by Hive ransomware,' 21 May 2022, https://www.bleepingcomputer.com/news/security/costa-rica-s-public-health-agency-hit-by-hive-ransomware/ and Chainalysis, 'DOJ and Europol announce disruption of Hive ransomware,' 26 January 2023, https://www.chainalysis.com/blog/hive-ransomware/.

[82] DOJ, 'US Department of Justice disrupts Hive ransomware variant,' 26 January 2023, https://www.justice.gov/archives/opa/pr/us-department-justice-disrupts-hive-ransomware-variant.

[83] Chainalysis, 'DOJ and Europol announce disruption of Hive ransomware.'

[84] DOJ, 'US Department of Justice disrupts Hive ransomware variant.'

[85] Christopher Wray, 'Remarks at press conference announcing the disruption of the Hive ransomware group,' 26 January 2023, https://www.fbi.gov/news/speeches-and-testimony/director-christopher-wrays-remarks-at-press-conference-announcing-the-disruption-of-the-hive-ransomware-group.

[86] In total, 12 countries and international organisations supported the operation. See: US Department of Justice, 'US Department of Justice disrupts Hive ransomware variant.'

[87] There is some dispute about the links between Hive and Hunters International. Some analysts identified technical and operational overlaps, as well as chatter on cybercriminal forums and marketplaces that suggest Hunters is run by the same operators as Hive; see:. Mahmoud Zohdy, Pietro Albuquerque, and Abzal Aitoriyev, 'The beginning of the end: the story of Hunters International,' Group-IB, 2 April 2025, https://www.group-ib.com/blog/hunters-international-ransomware-group/. Other analysts are more sceptical, although this seems to be largely based on Hunters International denying they are linked to Hive; see: Acronis Threat Research Unit, 'Hunters International: New ransomware based on Hive source code,' 1 July 2024, https://www.acronis.com/en/tru/posts/hunters-international-new-ransomware-based-on-hive-source-code/.

to deprive Hive's operators and affiliates of ransom revenue. The operation did not, however, strike directly at Hive's human and logistics network. Despite a US State Department reward for information of $10 million and the fact the operation apparently uncovered details on 250 Hive affiliates, no significant arrests, indictments, or sanctions have followed.[89]

Impact analysis

Severity: The severity of the operation against Hive was high. Following the takedown, Hive was never relaunched as a RaaS brand. Although Hive's administrators likely relaunched their operational activities as Hunters International, this did not happen until October 2023 – ten-months later.[90] More importantly, the operation affected Hive's operators and affiliates' ability to monetise ransomware for a six-month period before the infrastructure seizure. The Department of Justice estimated that the operation stopped as much as $130 million worth of ransom payments from being paid to Hive.[91] According to data collected by the cryptocurrency tracing company Chainalysis, Hive went from receiving the highest amount of known ransom payments in the second quarter of 2022 to almost nothing by the end of that year.[92] A former FBI official suggested that the operation, 'significantly degraded their ability to monetise, and we saw it. They were getting frustrated. Like, why are these guys not paying the ransom?'[93]

Scope: The operation against Hive also had a high impact in terms of its scope. This is in part due to the large number of victims the intervention helped, rather than its impact on operators and affiliates. In January 2023, US authorities assessed that the operation against Hive allowed them to generate and distribute decryption keys for as many as 1,300 victims.[94] While this number is difficult to verify and some affected organisations clearly continued to pay, it undoubtedly played a significant role in supporting a large number of victims.[95]

In terms of the ecosystem, the takedown of Hive in January 2023 removed one of the most prolific RaaS operations at the time. According to Coveware data, Hive had the largest market share of any ransomware strain in Q4 2022.[96] In fact, Hive's market share seems to have increased throughout 2022, even as victims started paying fewer ransoms to it. This may have contributed to a broader trend in

[88] DOJ, 'Deputy Attorney General Lisa O. Monaco Delivers Remarks on the Disruption of Hive Ransowmare Variant,' 26 January 2023, https://www.justice.gov/archives/opa/speech/deputy-attorney-general-lisa-o-monaco-delivers-remarks-disruption-hive-ransomware-variant.

[89] Sergiu Gatlan, 'US offers $10 million bounty for Hive ransomware links to foreign government,' *BleepingComputer*, 26 January 2023, https://www.bleepingcomputer.com/news/security/us-offers-10m-bounty-for-hive-ransomware-links-to-foreign-governments/; Sergiu Gatlan, 'French police arrests Russian suspect linked to Hive ransomware,' *BleepingComputer*, 13 December 2023, https://www.bleepingcomputer.com/news/security/french-police-arrests-russian-suspect-linked-to-hive-ransomware/.

[90] Martin Zugec, 'Hive Ransomware's Offspring: Hunters International takes the stage,' 9 November 2023, https://www.bitdefender.com/en-gb/blog/businessinsights/hive-ransomwares-offspring-hunters-international-takes-the-stage.

[91] DOJ, 'US Department of Justice disrupts Hive ransomware variant.'

[92] Chainalysis, 'DOJ and Europol announce disruption of Hive ransomware.'

[93] Authors' interview with former FBI official, 25 November 2025.

[94] DOJ, 'US Department of Justice disrupts Hive ransomware variant.'

[95] Chainalysis, 'DOJ and Europol announce disruption of Hive ransomware.'

the ransomware ecosystem in 2022 – the significant drop in the amount of ransom payments received by threat actors (from $983 million in 2021 to $567 million in 2022).[97] While other drivers, such as the demise of Conti and Russia's invasion of Ukraine, were likely more important, the counter-Hive operation still played a role. In 2023, a Chainalysis assessment said, 'we have attributed much of the drop in ransomware payments between 2021 and 2022 to victims' unwillingness to pay. … However, today's announcement indicates that this government action alone was a significant driver of the drop.'[98]

Longevity and reversibility: As noted, the Hive brand never relaunched. This suggests that, following law enforcement action and infrastructure compromise, re-establishing the brand was no longer seen as worthwhile, particularly given the availability of alternative paths for continuing operations under a different name. Indeed, in October 2023 a new RaaS brand with links to Hive emerged. Researchers quickly identified that Hunters International shared technical overlaps with Hive.[99] Although this could mean that Hunters International bought the source code from Hive, there are other indicators that link Hive's operators to Hunters International. According to the cyber threat intelligence vendor Group-IB, ransomware threat actors on cybercriminal forums frequently referred to Hunters International as Hive. Other threat actors claimed that they were contacted by Hunters International using an instant messaging account associated with Hive's administrators.[100] This suggests that Hive's operators continued to operate within the ransomware ecosystem. However, Coveware's reporting and ransomware data leak site monitoring highlights that Hunters International has never led the RaaS market in the way that Hive did in 2022.[101] It is difficult to assess whether this is because they were undermined by the intervention against Hive or for other reasons.

Signalling Value: The operation against Hive had a high impact in terms of its signalling value. This is primarily because of the signals it sent to ransomware victims. When announcing the operation against Hive, US officials stressed that it represented a new victim-centric approach. As Deputy Attorney General Lisa Monaco stated, the operation 'should speak as clearly to victims as it does to perpetrators'.[102] By stealing and distributing decryption keys, authorities demonstrated the potential of victims actively seeking alternatives to paying ransoms. This also demonstrated the value that law enforcement can deliver for victims and the public.

The operation also allowed law enforcement agencies to build on the interventions against REvil and

---

[96] Coveware, 'Improved security and backups result in record low number of ransomware payments,' January 2023, https://www.coveware.com/blog/2023/1/19/improved-security-and-backups-result-in-record-low-number-of-ransomware-payments.

[97] Chainalysis, 'Ransomware payments exceed $1 billion in 2023, hitting record high after 2022 decline, 7 February 2024, https://www.chainalysis.com/blog/ransomware-2024/.

[98] Chainalysis, 'DOJ and Europol announce disruption of Hive ransomware.'

[99] Martin Zugec, 'Hive Ransomware's Offspring: Hunters International takes the stage'..

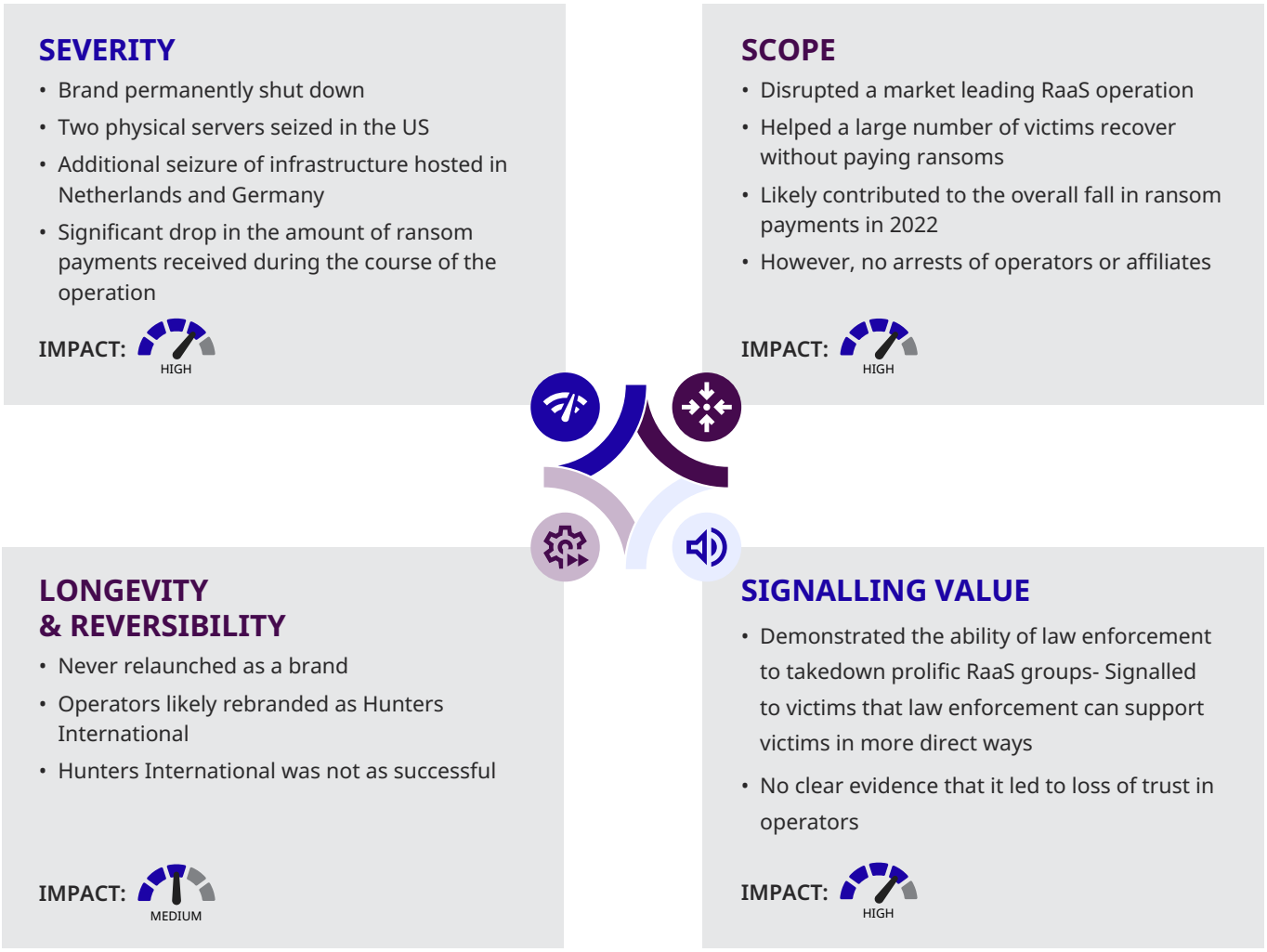
[100] Zohdy, Albuquerque, and Aitoriyev, 'The beginning of the end: the story of Hunters International'.

[101] See Coveware, 'Quarterly Reports' and Emsisoft, 'The state of ransomware in the US: report and statistics, 2025', 7 January 2026. https://www.emsisoft.com/en/blog/47215/the-state-of-ransomware-in-the-u-s-report-and-statistics-2025/.

[102] DOJ, 'US Department of Justice disrupts Hive ransomware variant.'

demonstrate their intent and capacity to disrupt market leading RaaS brands. This sent a signal that running a prolific, impactful RaaS operation can be damaging. In June 2023, a prominent ransomware analyst suggested that these kinds of interventions against RaaS operations could be fracturing the ransomware ecosystem, and pushing threat actors towards smaller, less high-profile groups.[103]

Figure 7: Impact Assessment Interventions against Hive



Interventions against Lockbit

For several years, from 2021 to 2024, Lockbit was one of the world's most active RaaS syndicates.[104] LockBit, however, began modestly in 2019 as a small, closed group using what responders dubbed the '.abcd virus', a strain that relied on basic email-based ransom demands and offered no public identity or leak site.[105]

---

[103] Allan Liska, 'Keynote: A post-apocalyptic hellscape – what ransomware looks like after Raas,' Sans Ransomware Summit, 23 June 2023, https://sansorg.egnyte.com/dl/4h5IJjdjly.

[104] According to Chainalysis, Lockbit's rank in terms of ransomware strain revenue was a follows: 8th in 2021, 4th in 2022, 2nd 2023, and once again 2nd in 2024.,'U.S. and U.K. Disrupt Lockbit Ransomware Group and Indict Two Russian Nationals While OFAC Levies Sanctions,' 21 February 2024, https://www.chainalysis.com/blog/lockbit-takedown-sanctions-february-2024/.

[105] ATR Operational Intelligence Team (co-authored by Marc RiveroLopez), 'Tales From the Trenches; a LockBit Ransomware Story,' McAfee Labs, 30 April 2020, https://www.mcafee.com/blogs/other-blogs/mcafee-labs/tales-from-the-trenches-a-lockbit-ransomware-story/.

LockBit shifted course in early 2020 with the launch of a new name and brand, LockBit 1.0, and reorientation of its operations around affiliates.[106] This transition introduced clearer branding, stricter targeting rules, and an unusually affiliate-friendly payment system which allowed affiliates to received ransom payments directly.[107] These changes helped LockBit attract operators seeking a more predictable and trustworthy arrangement than those offered by many rival groups.

LockBit 2.0, released in mid-2021, marked the group's significant expansion.[108] Although not the most active ransomware outfit, LockBit became one of the major players by introducing technical upgrades such as automated network-wide deployment, a proprietary data theft tool, and a more polished affiliate panel. The group broadened its reach to Linux and ESXi environments and attracted affiliates from disrupted groups like REvil and BlackMatter.[109] During this period, LockBit also invested heavily in its public image, running recruitment campaigns from its leak site, engaging directly with researchers, and adopting increasingly theatrical tactics to project stability and capability.[110]

With LockBit 3.0, the group further diversified its tooling and sharpened its brand. New variants such as LockBit Black and LockBit Green incorporated code from other families and expanded operating-system coverage, including an early macOS attempt.[111] LockBit added additional extortion layers, such as DDoS threats and paid options for delaying or deleting leaked data. Internally, it formalised roles, outsourced specialised functions, and continued to recruit affiliates from across the ransomware ecosystem.[112]

LockBit also leaned into high-visibility stunts – public bug bounties, media interactions, and even occasional apologies after controversial attacks – highlighting the group's combination technical adaptability with an unusually active public persona.[113]

In February 2024, an international task force of law enforcement agencies from at least ten countries, led by the UK's NCA and the FBI and code-named Operation Cronos, compromised Lockbit. 'In three

---

[106] The group openly advertised on darknet forums that 'ABCD ransomware was rebranded as LockBit in January 2020,' signalling to the criminal community that a new, more capable version was in circulation. Shunichi Imano and James Slaughter, 'Meet LockBit: The Most Prevalent Ransomware in 2022,' FortiGuard Labs, 10 July 2023, https://www.fortinet.com/blog/threat-research/lockbit-most-prevalent-ransomware.

[107] Intel 471, 'What Lies Ahead After LockBit's Disruption,' 20 February 2024, https://intel471.com/blog/what-lies-ahead-after-lockbits-disruption.

[108] Dmitry Smilyanets, 'An Interview With LockBit: The Risk of Being Hacked Ourselves Is Always Present,' *Record*, 30 September, 2021, https://therecord.media/an-interview-with-lockbit-the-risk-of-being-hacked-ourselves-is-always-present.

[109] CISA, FBI, Multi-State Information Sharing and Analysis Center (MS-ISAC), and international partners, 'Understanding Ransomware Threat Actors: LockBit,' 14 June 2023, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a; Imano and Slaughter, 'Meet LockBit: The Most Prevalent Ransomware.'

[110] For example, they publicly mocked and discredited REvil, Hive, and Alphv, accusing them of being unprofessional or unreliable: @AShukuhi (X), 'A Major Civil War in the Russian Cyber-Criminal Underground Between #LockBit, #Blackmatter, and Other Threat Actors,' 31 January 2022, https://x.com/AShukuhi/status/1488040262802812931; @ddd1ms (X), 'Another war on @xss_is forum between #LockBit and #ALPHV #ransomware,' 1 March 2022, https://x.com/ddd1ms/status/1496211830271840262.

[111] @vx-underground (X), 'Lockbit ransomware group has named Lockbit 3.0 as "Lockbit Black"' 23 May 2022, https://x.com/vxunderground/status/1528801206923141122; @vx-underground (X), 'Lockbit ransomware group announced today,' 26 June 2022, https://x.com/vxunderground/status/1541156954214727685.

[112] @PRODAFT (X), 'You asked and you shall receive,' 22 February 2024, https://x.com/PRODAFT/status/1760698932005388492.

[113] One bizarre stunt stands out: in early September 2022, LockBit offered cash rewards to anyone who tattooed the LockBit logo on their body. For a list of pictures see: 3xp0rt, 'LockBit-Tattoo GitHub Repository,' GitHub, 2022, https://github.com/3xp0rt/LockBit-Tattoo.

strikes', they wrote in the press release: 'by infiltrating their systems, and obtaining their data, taking control, and locking them out.'[114]

Targets of the intervention

On 19 February 2024, LockBit's Tor services suddenly fell under law enforcement control. Visiting LockBit's data leak site, users were now saw a banner reading: 'THIS SITE IS NOW UNDER THE CONTROL OF LAW ENFORCEMENT.'[115] The notice, branded with seals of various law enforcement agencies, declared the site was 'now under the control of the National Crime Agency of the UK, working in close cooperation with the FBI and the international law enforcement task force, "Operation Cronos".' It further stated: 'We can confirm that Lockbit's services have been disrupted as a result of International Law Enforcement action – this is an ongoing and developing operation. Return here for more information at: 11:30 GMT on Tuesday 20th Feb.'[116]

The next day, on 20 February, law enforcement repurposed LockBit's own website to publish a trove of information about the group. The NCA and its partners replaced the group's usual leak pages with a multi-lingual exposé of LockBit's inner workings. This included posting decryption keys (so past victims could unlock their files for free), a rundown of LockBit's tactics and software, and even a 'wanted' notice offering a $10 million reward for information on LockBitSupp, the group's leader. Law enforcement was essentially trolling Lockbit by using its own platform to reveal its secrets.[117] Operation Cronos stands out because it is a rare law enforcement campaign that hit all three ransomware pillars: technical capacity, organisational structure, and public perception.

At the core of Operation Cronos was the technical takedown of servers and tools. Investigators had secretly obtained access to LockBit's primary servers, including those hosting its blog, negotiation portal, and 'StealBit', the group's bespoke exfiltration tool.[118] In total, at least 34 servers distributed across multiple countries were seized or knocked offline.[119] By seizing servers, the authorities effectively 'destroyed the online backbone of the LockBit group', as US Deputy Attorney General Lisa Monaco put it.[120] Furthermore, the NCA put out a message for victims: 'If you've been impacted by LockBit, we now have 1000 decryption keys taken from LockBit's site to help you decrypt stolen data.' They provided UK and US contact details and a link to the No More Ransom website.[121] Operation

[114] NCA, 'The NCA Announces the Disruption of LockBit With Operation Cronos,' 20 February 2024, https://www.nationalcrimeagency.gov.uk/the-nca-announces-the-disruption-of-lockbit-with-operation-cronos.

[115] NCA, 'LockBit Leader Unmasked and Sanctioned,' 7 May 2024, https://www.nationalcrimeagency.gov.uk/news/lockbit-leader-unmasked-and-sanctioned.

[116] *Ibid.*

[117] NCA, 'The NCA Announces the Disruption of LockBit With Operation Cronos.'

[118] *Ibid.*

[119] This was in the Netherlands, Germany, Finland, France, Switzerland, Australia, the United States and the United Kingdom. See: Europol, 'Law Enforcement Disrupt World's Biggest Ransomware Operation,' 30 May 2024, https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation.

[120] DOJ, 'U.S. and U.K. Disrupt LockBit Ransomware Variant,' 20 February 2024, https://www.justice.gov/archives/opa/pr/us-and-uk-disrupt-lockbit-ransomware-variant.

[121] No More Ransom Project, 'Decryption Tools,' accessed 19 January 2026, https://www.nomoreransom.org/en/decryption-tools.html.

Cronos also struck at Lockbit's finances: over 200 cryptocurrency wallets linked to the organisation were identified and frozen.[122]

The infiltration also allowed the NCA and its partners to disrupt LockBit's organisational structure. Law enforcement authorities obtained information on the group's network of almost 200 affiliates and published all affiliate IDs and usernames online.[123] Operation Cronos also resulted in arrests, with two individuals linked to LockBit detained in Poland and Ukraine. In addition, French and US authorities issued three international arrest warrants and filed five indictments. More than 14,000 accounts tied to LockBit's data theft activities and supporting infrastructure were also taken offline. The operation further exposed the group's administrator and developer, Russian national Dmitry Khoroshev, who was subsequently sanctioned. As the NCA press release read, 'Khoroshev, AKA LockBitSupp, who thrived on anonymity and offered a $10 million reward to anyone who could reveal his identity, will now be subject to a series of asset freezes and travel bans. US partners have also unsealed an indictment against him and are offering a reward of up to $10m for information leading to his arrest and/or conviction.'[124]

Finally, Operation Cronos stood out because it went after LockBit's brand directly.[125] As noted earlier, the NCA hijacked LockBit's leak site and replaced its content, even mirroring LockBit's colour scheme, fonts, and ransom-style countdown clock. But, more importantly, law enforcement used the takeover to highlight how LockBit had repeatedly broken its promises. Victims had been told their stolen data would be deleted after payment; the NCA showed this was false. LockBit also claimed to enforce strict rules on its members, yet Cronos revealed affiliates continued launching attacks despite these supposed constraints.

Impact analysis

Severity: Operation Cronos delivered a severe blow to LockBit, unprecedented in scope for a ransomware takedown. Unlike earlier actions against ransomware groups, which often yielded arrests or a website seizure, but not both, Cronos was a comprehensive strike at every level of LockBit's enterprise. From a law enforcement perspective, Cronos was one of the most – if not, the most – significant cyber takedowns ever.

Scope: The impact of Operation Cronos reverberated far beyond LockBit itself. By targeting such a large RaaS operation, law enforcement indirectly affected the broader ransomware ecosystem. First, many LockBit affiliates also dabbled in other RaaS programs; those actors faced uncertainty and doubt about whether their identities had been compromised. Second, the intelligence gathered by Cronos bridged connections between criminal groups. According to

[122] Global Initiative Against Transnational Organized Crime, "The LockBit Takedown: Law Enforcement Trolls Ransomware Gang," February 2024, https://globalinitiative.net/analysis/the-lockbit-takedown-law-enforcement-trolls-ransomware-gang/

[123] NCA, 'The NCA Announces the Disruption of LockBit With Operation Cronos.'

[124] NCA, 'LockBit Leader Unmasked and Sanctioned.'

[125] This is also well highlighted in Matt Burgess, 'The Notorious LockBit Ransomware Gang Has Been Disrupted by Law Enforcement,' *Wired*, 20 February 2024, https://www.wired.com/story/lockbit-ransomware-takedown-website-nca-fbi.

Prodraft, Operation Cronos provided 'in-depth visibility into each affiliate's structures, including ties with other notorious groups such as FIN7, Wizard Spider, and EvilCorp'.[126]

Longevity and reversibility: Operation Cronos achieved a durable reduction in LockBit's operational viability. While not an absolute eradication, the intervention inflicted a debilitating blow, from which meaningful recovery proved extremely difficult. LockBit's dominance within the ransomware ecosystem effectively ended.[127]

LockBit had previously weathered significant setbacks – most notably a 2022 source code leak – and had returned stronger. Following Operation Cronos, elements of the operation briefly reappeared, including the rapid establishment of a new leak site and the launch of LockBit 4.0. The significance of this re-emergence, however, lies less in its occurrence than in its limited scale and performance.

LockBit 4.0 was active for a brief period before its internal platform was leaked. This sequence provides a rare opportunity for direct comparison with earlier iterations of the same operation. The available data indicate that LockBit's post-Cronos incarnation was a hollowed-out version of its former self. Between December 2024 and April 2025, LockBit 4.0 registered roughly 75 affiliate accounts, a sharp decline from the approximately 200 affiliates active under LockBit 3.0 between May 2022 and February 2023. Of those 75 affiliates, only 35 entered negotiations with a victim, and just eight ultimately received ransom payments. By contrast, around 80 affiliates were paid under LockBit 3.0, which was associated with more than 600 victims overall. Based on available evidence, only around 19 victims are estimated to have paid LockBit 4.0.[128]

Contemporaneous assessments by authorities support this analysis. The NCA and partner agencies assessed that LockBit's remaining team was 'running at limited capacity' following the operation.[129] As Jack Meegan-Vickers notes, the public spectacle of Cronos – including the defacement of the leak site, the exposure of broken promises, and the identification of the group's leader – 'certainly caused irreparable damage' to LockBit's brand equity.[130]

Signalling Value: While operations like REvil and Hive had already eroded the sense of invincibility among ransomware crews, Operation Cronos expanded the psychological pressure by combining infrastructure takedown, decryption key recovery, and public humiliation in one coordinated campaign.

---

[126] @PRODAFT (X), 'Since LOCKBIT's first entry into the cybercrime ecosystem,' 20 February 2024, https://x.com/prodaft/status/1759906800311157066?s=46&t=FA8la2ipfsQG7kSh21skxQ.

[127] The LockBitSupp persona's post-operation statements tried to preserve LockBit's credibility, claiming the group was 'lazy' and would return stronger, but most analysts read these as damage control. Their new 'LockBit 4.0' leak site posted old breaches to simulate activity, undermining their own message of continuity.

[128] For a more detailed comparison between Lockbit 3.0 and 4.0 based on the leaked data see: Max Smeets, *Inside the Ransomware Machine*, Keynote: Black Hat Europe 2026, 10 December 2025.

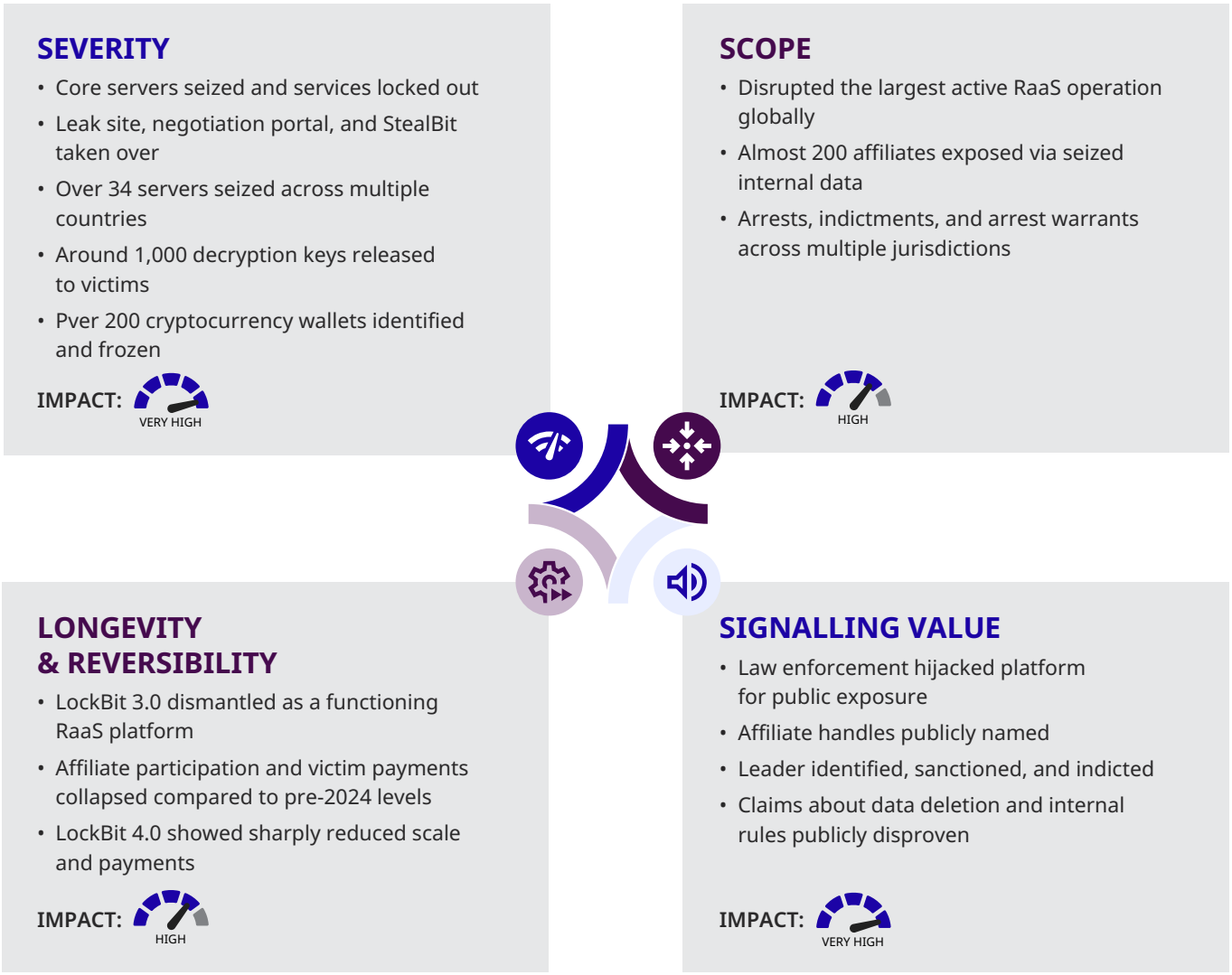
[129] NCA, 'LockBit Leader Unmasked and Sanctioned.'

[130] Jack Meegan-Vickers, 'The LockBit Takedown: Law Enforcement 'Trolls' Ransomware Gang,' Global Initiative Against Transnational Organized Crime, 4 April 2024, https://globalinitiative.net/analysis/the-lockbit-takedown-law-enforcement-trolls-ransomware-gang/.

This reframing of perception extended to LockBit affiliates. The NCA's unusual choice to post usernames of known affiliates on the seized site was aimed at seeding paranoia. Affiliates were told, 'We know who you are.' This was not just about legal threat – it was about shaking the foundations of trust that LockBit relied on to function as a service platform.

In short, Operation Cronos weaponised visibility. It added a public-facing – almost theatrical - dimension that amplified the signalling value across the criminal ecosystem. It then was careful about its messaging about the untrustworthiness of Lockbit, with further ramifications in the ransomware ecosystem. Other ransomware groups may have since found it harder to get paid out, as negotiators could point to the fact that Operation Cronos had shown that data would not always be deleted.[131]

Figure 8: Impact Assessment Interventions against Lockbit



[131] Blavatnik School of Government and European Cyber Conflict Research Initiative (ECCRI), 'The Oxford Cyber Forum: A Dialogue on the Evolving Landscape of Cyber Conflict and Security,' 27 June 2024, https://www.bsg.ox.ac.uk/events/oxford-cyber-forum.

DISCUSSION

A recurring challenge in counter-ransomware policy is the tendency to equate visibility with effectiveness. Highly visible interventions – particularly those accompanied by coordinated media messaging – are often treated as inherently successful. As the framework developed in this report shows, however, visibility is not a reliable proxy for impact. Public prominence may generate reassurance, deterrent signalling, or political value, but these effects do not automatically translate into sustained disruption of ransomware activity. The framework helps disaggregate these dynamics, making clear that attention and impact are analytically distinct.

> Visibility is not a reliable proxy for impact.

When applied across cases, the framework reveals a consistent impact profile. Many interventions score relatively highly on severity, and increasingly high on signalling value, particularly where operations involve infrastructure seizures, leak-site disruptions, arrests, or public attribution. By contrast, these same interventions often struggle to achieve comparable on longevity. Ransomware actors can rebuild infrastructure, migrate affiliates, or rebrand with relative speed, meaning that sharp operational shocks are frequently reversible. Without follow-on actions or complementary measures, even severe disruptions may translate into only short-lived reductions in activity. The framework makes these trade-offs visible, allowing analysts to distinguish between immediate disruption and durable change.

The comparative case analysis shows that different intervention types produce distinct impact profiles rather than uniform outcomes. Operations targeting shared technical enablers, such as Emotet, generate very high scope of impact and immediate disruption across the ecosystem, but are also prone to substitution effects as alternative services rapidly fill the gap. Actor-focused interventions, such as those against REvil, can inflict severe and lasting damage on a specific brand or organisational network, yet still produce only moderate ecosystem-wide effects as affiliates and capabilities migrate elsewhere.

> Operation Cronos stands out because it combined infrastructure takedown, organisational exposure, and reputational disruption in a single campaign, resulting in high scores across all four impact dimensions and observable post-intervention degradation.

Across the cases, durability appears to depend less on the initial shock than on whether interventions constrain reconstitution. Longevity is strongest where authorities create sustained uncertainty for operators, degrade internal trust relationships, and limit the ability to rebuild at scale. This includes persistent fears of ongoing access or compromise, the exposure of affiliates and intermediaries, and follow-on measures that reinforce earlier disruption. Interventions that undermine the brand and reputation of individual operators and administrators rather than just the services and brands they maintain are also more likely to have a long-term impact. If affiliates lose trust in an indicted, sanctioned RaaS operator, for example, it makes it considerably harder for that operator to successfully run operations at scale. In contrast, one-off actions – even when severe – are more likely to be absorbed by the ecosystem over time.

> Across the cases, durability appears to depend less on the initial shock than on whether interventions constrain reconstitution.

The report has deliberately avoided ranking ecosystem-level targeting above actor-centric targeting. Instead, the framework shows that these approaches generate different kinds of impact. Actor-centric interventions often produce sharp but narrow effects, incapacitating a specific group, disrupting trust relationships, or removing key individuals. Ecosystem-level interventions – targeting shared services, access brokers, or laundering networks – tend to produce broader scope and greater longevity, but may lack immediacy or visibility. In practice, an effective long-term counter-ransomware intervention is likely to require both. The analytical value of the framework lies in

making these differences explicit, rather than collapsing them into a single measure of success.

Another insight is that impact is not unambiguously positive. Interventions do not merely suppress activity; they reshape the ransomware ecosystem. One example concerns sustained pressure on large RaaS operations. Targeting dominant platforms can fragment the market, leading to a proliferation of smaller groups and brands. In the short term, this dispersion may be beneficial: activity becomes less concentrated, brands are weaker, and coordination costs rise. Initial data suggest that such fragmentation can reduce efficiency and trust within the ecosystem.

Over longer time horizons, however, these effects may undermine objectives. A more fragmented ecosystem may generate greater experimentation, faster learning across multiple independent groups, and increased difficulty for defenders seeking to monitor activity systematically. Fragmentation can also complicate attribution and prioritisation. The framework does not resolve whether these ecosystem shifts are ultimately desirable, but it does surface them explicitly, highlighting that interventions can generate second- and third-order effects that evolve over time.

Recent interventions also highlight the growing depth of cooperation between law enforcement and private-sector actors. This collaboration has enabled a series of operational successes, particularly where private firms provide technical access, telemetry, and analytical capabilities that governments alone do not possess. Operation Endgame illustrates this dynamic clearly, combining multinational law enforcement coordination with sustained private-sector involvement across multiple phases of disruption. Such partnerships have expanded the range of feasible countermeasures and increased the scale at which interventions can be executed.

At the same time, this model introduces incentives that warrant caution. Shared interests in demonstrating relevance, effectiveness, or return on investment can encourage optimistic narratives about impact. Where many law enforcement and private sector actors are publicly associated with an intervention, there may be fewer incentives to surface critical assessments or to acknowledge limited or reversible effects. The framework provides a counterweight to this tendency by offering a structured way to assess impact beyond claims of participation or visibility, helping to reintroduce analytical discipline into post-operation evaluation.

Finally, the application of the framework underscores the limits of (perfect) measurement in this domain. Data asymmetries persist across jurisdictions and between public and private actors, while classification barriers restrict access to key operational details. These limitations cannot be eliminated. However, transparent, structured judgments grounded in clearly defined dimensions are still preferable to intuitive, ad hoc evaluation. The framework's value thus lies in its consistency and comparability.

CONCLUSION

This report addresses a persistent gap in counter-ransomware policy: the absence of a shared, indicator-based framework for assessing the impact of interventions and countermeasures. In response, it introduces a framework that distinguishes between severity, scope, longevity and reversibility, and signalling value. Together, these dimensions provide a structured way to describe and compare impact across ransomware interventions.

The first implication is strategic. Counter-ransomware efforts benefit from greater clarity about what kind of change an intervention is intended to produce. Too often, interventions are discussed in terms of the tools deployed rather than the effects sought, with success assessed only retrospectively. By separating different dimensions of impact, the framework encourages policymakers to think explicitly about whether an intervention aims for narrow or broad effects, immediate disruption or enduring change, and direct operational damage or wider ecosystem signalling. Not all interventions should seek high impact across all dimensions; limited or targeted effects may be appropriate. What matters is that these choices are explicit.

> “This report addresses a persistent gap in counter-ransomware policy: the absence of a shared, indicator-based framework for assessing the impact of interventions and countermeasures.”

The second implication is organisational. Impact assessment should be treated as a continuous practice embedded in operations, rather than as a one-off evaluation. Applied iteratively – through an initial impact profile, a minimum common dataset, and follow-up assessments at set intervals – the framework can capture adaptation, displacement, and recovery. Over time, this supports learning across cases, helps identify which combinations of countermeasures tend to produce more durable effects, and enables more deliberate sequencing of interventions. The aim is not perfect measurement, but institutional learning that shifts counter-ransomware strategy from episodic success towards cumulative, ecosystem-level pressure.

REFERENCES

@AShukuhi. 'A Major Civil War in the Russian Cyber-Criminal Underground Between #LockBit, #Blackmatter, and Other Threat Actors.' *Thread Reader App*, 31 January 2022. https://threadreaderapp.com/thread/1488040262802812931.html.

@ddd1ms. 'Another War on @xss_is Forum Between #LockBit and #ALPHV #Ransomware.' X, 1 March 2022. https://x.com/ddd1ms/status/1496211830271840262.

@PRODAFT. 'Since LOCKBIT's First Entry into the Cybercrime Ecosystem.' X, 20 February 2024. https://x.com/prodaft/status/1759906800311157066.

@PRODAFT. 'You Asked and You Shall Receive.' X, 22 February 2024. https://x.com/PRODAFT/status/1760698932005388492.

@snatch_info. Post no. 193. *Telegram*, accessed 19 January 2026. https://t.me/snatch_info/193.

@vx-underground. 'Lockbit ransomware group has named Lockbit 3.0 as "Lockbit Black,"' X, 23 May 2022. https://x.com/vxunderground/status/1528801206923141122.

@vx-underground. 'Lockbit ransomware group announced today,' X, 26 June 2022. https://x.com/vxunderground/status/1541156954214727685.

3xp0rt, 'LockBit-Tattoo GitHub Repository,' GitHub, 2022, https://github.com/3xp0rt/LockBit-Tattoo.

Abrams, Lawrence. 'Another Ransomware Will Now Publish Victims' Data If Not Paid.' 12 December 2019. https://www.bleepingcomputer.com/news/security/another-ransomware-will-now-publish-victims-data-if-not-paid/.

Abrams, Lawrence. "Sodinokibi Ransomware Says Travelex Will Pay, One Way or Another." *BleepingComputer*, 9 January 2020. https://www.bleepingcomputer.com/news/security/sodinokibi-ransomware-says-travelex-will-pay-one-way-or-another/.

Adams, Lawrence. 'REvil ransomware deposits $1 million in hacker recruitment drive.' *Bleeping Computer*, 28 September 2020. https://www.bleepingcomputer.com/news/security/revil-ransomware-deposits-1-million-in-hacker-recruitment-drive/.

Adam M, 'The Evolution of PINCHY SPIDER from GandCrab to REvil,' *CrowdStrike*, 7 July 2021, https://www.crowdstrike.com/en-us/blog/the-evolution-of-revil-ransomware-and-pinch

Acronis Threat Research Unit, 'Hunters International: New ransomware based on Hive source code,' Acronis, 1 July 2024, https://www.acronis.com/en/tru/posts/huntersinternational-new-ransomware-based-on-hive-source-code/.

Alperovitch, Dimitri. 'REvil is down – for now,' Lawfare, November 16, 2021, https://www.lawfaremedia.org/article/revil-down-now

ATR Operational Intelligence Team (co-authored by Marc RiveroLopez), 'Tales From the Trenches; a LockBit Ransomware Story,' McAfee Labs, 30 April 2020, https://www.mcafee.com/blogs/other-blogs/mcafee-labs/talesfrom-the-trenches-a-lockbit-ransomware-story/.

BBC News, 'Meat Giant JBS Pays $11m in Ransom to Resolve Cyber-Attack,' 10 June 2021, https://www.bbc.co.uk/news/business-57423008.

BBC News, 'REvil ransomware gang arrested in Russia,' 14 January 2022, https://www.bbc.co.uk/news/technology-59998925.

Blavatnik School of Government and European Cyber Conflict Research Initiative (ECCRI), 'The Oxford Cyber Forum: A Dialogue on the Evolving Landscape of Cyber Conflict and Security,' June 27, 2024, https://www.bsg.ox.ac.uk/events/oxford-cyber-forum

Burgess, Matt, 'The Notorious LockBit Ransomware Gang Has Been Disrupted by Law Enforcement,' WIRED, February 20, 2024,https://www.wired.com/story/lockbit-ransomware-takedown-website-nca-fbi

Cimpanu, Catalin. 'Authorities Plan to Mass-Uninstall Emotet From Infected Hosts on April 25, 2021,' *ZDNet*, 27 January 2021, https://www.zdnet.com/article/authorities-plan-to-mass-uninstall-emotet-from-infected-hosts-on-april-25-2021/.

Chainalysis, 'DOJ and Europol announce disruption of Hive ransomware,' 26 January 2023, https://www.chainalysis.com/blog/hive-ransomware/.

Chainalysis, 'Ransomware payments exceed $1 billion in 2023, hitting record high after 2022 decline,' 7 February 2024, https://www.chainalysis.com/blog/ransomware-2024/.

Chainalysis,'US and UK Disrupt Lockbit Ransomware Group and Indict Two Russian Nationals While OFAC Levies Sanctions,' February 21, 2024, https://www.chainalysis.com/blog/lockbit-takedown-sanctions-february-2024/.

Coveware, 'Improved security and backups result in record low number of ransomware payments,' January 2023, https://www.coveware.com/blog/2023/1/19/improved-security-and-backups-result-in-record-low-number-of-ransomware-payments.

Coveware, 'Quarterly Reports,' https://www.coveware.com/ransomware-quarterly-reports.

Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), Multi-State Information Sharing and Analysis Center (MS-ISAC), and international partners. 'Understanding Ransomware Threat Actors: LockBit,' June 14, 2023, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a

Cybersecurity and Infrastructure Security Agency (CISA) and Federal Bureau of Investigation (FBI). "#StopRansomware: Snatch Ransomware," September 20, 2023, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-263a

De Moura, Georges, and Tal Goldstein. 'What the Biden-Putin Summit Reveals about Future of Cyber Attacks – and How to Increase Cybersecurity.' *World Economic Forum*, 17 June 2021. https://www.weforum.org/agenda/2021/06/joe-biden-vladimir-putin-summit-cybersecurity/.

DiMaggio, Jon. 'A History of REvil.' *Analyst1*, accessed 6 May 2024. https://analyst1.com/history-of-revil/.

Ducklin, Paul. 'Kaseya Ransomware Attackers Say: "Pay $70 Million and We'll Set Everyone Free."' 5 July 2021. https://www.sophos.com/it-it/blog/kaseya-ransomware-attackers-say-pay-70-million-and-well-set-everyone-free/.

Emsisoft. 'The state of ransomware in the US: report and statistics, 2025.' 7 January 2026. https://www.emsisoft.com/en/blog/47215/the-state-of-ransomware-in-the-u-s-report-and-statistics-2025/.

ESET Research. 'ESET Research Follows the Comeback of the Infamous Botnet Emotet, Targeting Mainly Japan and South Europe,' 6 July 2023. https://www.eset.com/us/about/newsroom/press-releases/eset-research-follows-the-comeback-of-the-infamous-botnet-emotet/.

Europol. 'World's Most Dangerous Malware EMOTET Disrupted Through Global Action,' January 27, 2021, https://www.europol.europa.eu/media-press/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action.

Europol. 'Largest Ever Operation Against Botnets Hits Dropper Malware Ecosystem,' 30 May 2024. https://www.europol.europa.eu/media-press/newsroom/news/largest-ever-operation-against-botnets-hits-droppermalware-ecosystem.

Europol. 'Law Enforcement Disrupt World's Biggest Ransomware Operation,' 30 May 2024. https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomwareoperation.

Europol.'OperationENDGAMEStrikesAgain:theRansomwareKillChainBrokenatItsSource,'23May2025.https://www.europol.europa.eu/media-press/newsroom/news/operation-endgame-strikes-again-ransomware-kill-chain-broken-its-source.

Federal Bureau of Investigation. IC3 Alert: *Indicators of Compromise Associated with Hive Ransomware (TLP:WHITE)*, 25 August 2021. https://www.ic3.gov/CSA/2021/210825.pdf.

Federal Bureau of Investigation. 'Operation Endgame: Coordinated Worldwide Law Enforcement Action Against Network of Cybercriminals,' 30 May 2024. https://www.fbi.gov/news/press-releases/operationendgame-coordinated-worldwide-law-enforcement-action-against-network-of-cybercriminals.

Fokker, John. 'Dismantling a Prolific Cybercriminal Empire: REvil Arrests and Reemergence.' *Trellix*, 29 September 2022. https://www.trellix.com/en-gb/blogs/research/dismantling-a-prolific-cybercriminal-empire/.

FSB of Russia. 'Illegal Activities of Members of the Organized Criminal Community Were Suppressed,' Federal Security Service of the Russian Federation, January 14, 2022, http://www.fsb.ru/fsb/press/message/single.htm%21id%3D10439388%40fsbMessage.html.

Gatlan, Sergiu. 'Costa Rica's Public Health Agency Hit by Hive Ransomware.' 21 May 2022. https://www.bleepingcomputer.com/news/security/costa-rica-s-public-health-agency-hit-by-hive-ransomware/.

Gatlan, Sergiu. 'US Offers $10 Million Bounty for Hive Ransomware Links to Foreign Government.' *BleepingComputer*, 26 January 2023. https://www.bleepingcomputer.com/news/security/us-offers-10m-bounty-for-hive-ransomware-links-to-foreign-governments/.

Gatlan, Sergiu. 'French Police Arrests Russian Suspect Linked to Hive Ransomware.' BleepingComputer, 13 December 2023. https://www.bleepingcomputer.com/news/security/french-police-arrests-russian-suspect-linked-to-hive-ransomware/.

Global Initiative Against Transnational Organized Crime, "The LockBit Takedown: Law Enforcement Trolls Ransomware Gang," February 2024, https://globalinitiative.net/analysis/the-lockbit-takedown-law-enforcement-trolls-ransomware-gang/

Greig, Jonathan. 'FBI Decision to Withhold Kaseya Ransomware Decryption Keys Stirs Debate.' *ZDNET*, 24 September 2021. https://www.zdnet.com/article/fbi-decision-to-withhold-kaseyaransomware-decryption-keys-stirs-debate/.

Greig, Jonathan. 'Snatch Gang "Consistently Evolved" in Targeting Multiple Industries, Feds Say.' *The Record from Recorded Future News*, 20 September 2023. https://therecord.media/snatch-ransomware-group-alert-fbi-cisa.

Hakmeh, Joyce, and Jamie Saunders. 'The Strategic Approach to Countering Cybercrime (SACC) Framework.' *Chatham House*, July 2024. https://www.chathamhouse.org/2024/07/strategic-approach-countering-cybercrime-saccframework.

Healey, Jason, Neil Jenkins, and JD Work. 'Defenders Disrupting Adversaries: Framework, Dataset, and Case Studies of Disruptive Counter-Cyber Operations.' *12th International Conference on Cyber Conflict (CyCon)*, 2020. https://www.ccdcoe.org/uploads/2020/05/CyCon_2020_14_Healey_Jenkins_Work.pdf.

Holland, Steve, and Andrea Shalal. 'Biden Presses Putin to Act on Ransomware Attacks, Hints at Retaliation.' Reuters, 10 July 2021. https://www.reuters.com/technology/biden-pressed-putin-call-act-ransomware-attacks-white-house-2021-07-09/.

Ilascu, Ionut. 'REvil Ransomware Found Buyer for Trump Data, Now Targeting Madonna.' *BleepingComputer*, 18 May 2020. https://www.bleepingcomputer.com/news/security/revil-ransomware-found-buyer-for-trump-data-now-targeting-madonna/.

Ilascu, Ionut. 'US Seizes $6 Million from REvil Ransomware, Arrest Kaseya Hacker.' *BleepingComputer*, 8 November 2021. https://www.bleepingcomputer.com/news/security/us-seizes-6-million-from-revil-ransomware-arrest-kaseyahacker/.

Imano, Shunichi, and James Slaughter. 'Meet LockBit: The Most Prevalent Ransomware in 2022.' *FortiGuard Labs*, 10 July 2023. https://www.fortinet.com/blog/threat-research/lockbit-most-prevalent-ransomware.

Intel 471, 'What Lies Ahead After LockBit's Disruption,' February 20, 2024, https://intel471.com/blog/what-liesahead-after-lockbits-disruption

Interpol. 'A Comparative Threat Assessment on Counter Ransomware Interventions,' October 20, 2025, https://members.counter-ransomware.org/documents.

Kivilevich, Victoria. 'Will the REvil Story Finally Be Over?' 25 October 2021. https://www.kelacyber.com/blog/will-the-revil-story-finally-be-over/.

Lakshmanan, Ravie. 'European Authorities Disrupt Emotet — World's Most Dangerous Malware,' 28 January 2021. https://thehackernews.com/2021/01/european-authorities-disrupt-emotet.html.

Lakshmanan, Ravie. '300 Servers and €3.5M Seized as Europol Strikes Ransomware Networks Worldwide,' 23 May 2025. https://thehackernews.com/2025/05/300-servers-and-35m-seized-as-europol.html.

Larson, Selena, Daniel Blackford, and Garrett G. 'The First Step: Initial Access Leads to Ransomware.' *Proofpoint*, 16 June 2021. https://www.proofpoint.com/us/blog/threat-insight/first-step-initial-access-leads-ransomware.

Lawrence, Abrams. 'REvil Ransomware's Servers Mysteriously Come Back Online.' *BleepingComputer*, 7 September 2021. https://www.bleepingcomputer.com/news/security/revil-ransomwares-servers-mysteriously-come-back-online/.

Lawrence, Abrams. 'REvil Ransomware Shuts Down Again after Tor Sites Were Hijacked.' *BleepingComputer*, 17 October 2021. https://www.bleepingcomputer.com/news/security/revil-ransomware-shuts-down-again-after-torsites-were-hijacked/.

Liska, Allan, 'Keynote: A post-apocalyptic hellscape – what ransomware looks like after Raas,' Sans Ransomware Summit, 23 June 2023, https://sansorg.egnyte.com/dl/4h5IJjdjly.

MacColl, Jamie, Pia Hüsch, Gareth Mott, James Sullivan, Jason R. C. Nurse, Sarah Turner, and Nandita Pattnaik. 'The Scourge of Ransomware: Victim Insights on Harms to Individuals, Organisations and Society.' *RUSI Occasional Paper*, January 2024 (Royal United Services Institute for Defence and Security Studies, 2024). https://static.rusi.org/ransomware-harms-op-january-2024.pdf.

Malwarebytes Labs, 'Pow! Emotet's Down. Is It Out?' January 27, 2021, https://www.malwarebytes.com/blog/news/2021/01/emotets-down-is-it-out.

Martin, Alexander. 'Emotet: Police Raids Take Down Botnet That Hacked "Millions of Computers Worldwide."' *Sky News*, 27 January 2021. https://news.sky.com/story/emotet-police-raids-take-down-botnet-that-hacked-millions-of-computers-worldwide-12200460.

Meegan-Vickers, Jack. 'The LockBit Takedown: Law Enforcement "Trolls" Ransomware Gang.' *Global Initiative Against Transnational Organized Crime*, 4 April 2024. https://globalinitiative.net/analysis/the-lockbit-takedown-law-enforcement-trolls-ransomware-gang/.

National Crime Agency (NCA). 'The NCA Announces the Disruption of LockBit With Operation Cronos,' 20 February 2024. https://www.nationalcrimeagency.gov.uk/the-nca-announces-the-disruption-of-lockbit-with-operation-cronos.

National Crime Agency (NCA). 'LockBit Leader Unmasked and Sanctioned,' 7 May 2024. https://www.nationalcrimeagency.gov.uk/news/lockbit-leader-unmasked-and-sanctioned.

National Crime Agency (NCA). 'Annual Report and Accounts 2024-2025,' July 29, 2025, https://www.gov.uk/government/publications/national-crime-agency-annual-report-and-accounts-2024-to-2025.

Nakashima, Ellen, and Rachel Lerman. 'FBI Held Back Ransomware Decryption Key from Businesses to Run Operation Targeting Hackers.' *The Washington Post*, 21 September 2021. https://www.washingtonpost.com/national-security/ransomware-fbi-revil-decryption-key/2021/09/21/4a9417d0-f15f11eb-a452-4da5fe48582d_story.html.

Nakashima, Ellen, and Dalton Bennett. 'A Ransomware Gang Shut Down after Cybercom Hijacked Its Site and It Discovered It Had Been Hacked.' *The Washington Post*, 3 November 2021. https://www.washingtonpost.com/national-security/cyber-command-revil-ransomware/2021/11/03/528e03e6-3517-11ec-9bc4-86107e7b0ab1_story.html.

Nakashima, Ellen and Dalton Bennett, 'Ring of Ransomware Hackers Targeted by Authorities in United States and Europe,' The Washington Post, November 11, 2021, https://www.washingtonpost.com/national-security/revilransomware-arrests-doj/2021/11/08/9432dfc2-409f-11ec-a88e-2aa4632af69b_story.html.

Nechepurenko, Ivan. 'Russia Says It Shut Down Notorious Hacker Group at US Request.' *The New York Times,* 14 January 2022, sec. World, accessed 7 May 2024. https://www.nytimes.com/2022/01/14/world/europe/revil-ransomware-russia-arrests.html.

No More Ransom Project. 'Decryption Tools.' Accessed 19 January 2026. https://www.nomoreransom.org/en/decryption-tools.html.

OECD. 'Evaluation Criteria,' 2025. https://www.oecd.org/en/topics/sub-issues/development-co-operation-evaluation-and-effectiveness/eva.

Quinn, James. 'Emotet Evolves with New Wi-Fi Spreader.' Binary Defense, accessed 19 January 2026. https://binarydefense.com/resources/blog/emotet-evolves-with-new-wi-fi-spreader/.

RaphaelSatter,'HackersDemand$70MilliontoLiberateDataHeldbyCompaniesHitinMassCyberattack,'5July2021.https://www.reuters.com/technology/hackers-demand-70-million-liberate-data-held-by-companies-hit-mass-cyberattack-2021-07-05/.

Smilyanets, Dmitry. 'I Scrounged through the Trash Heaps… Now I'm a Millionaire: An Interview with REvil's J Unknown.' *The Record*, 16 March 2021. https://therecord.media/i-scrounged-through-the-trash-heaps-now-im-amillionaire-an-interview-with-revils-unknown.

Smilyanets, Dmitry. 'An Interview With LockBit: The Risk of Being Hacked Ourselves Is Always Present.' *The Record from Recorded Future News*, 30 September 2021. https://therecord.media/an-interview-with-lockbit-the-risk-of-being-hacked-ourselves-is-always-present.

Smeets, Max. Ransom War: *How Cyber Crime Became a Threat to National Security*. Oxford University Press, 2025.

Smeets, Max. Inside the Ransomware Machine, Keynote: Black Hat Europe 2026, 8–11 December 2025.

Spamhaus Team, 'Emotet Infrastructure Disrupted After Coordinated Action,' 29 January 2021. https://www.spamhaus.org/resource-hub/malware/emotet-infrastructuredisrupted-after-coordinated-action/.

US–Russia Summit. 'US President Joe Biden and Russian President Vladimir Putin Meet in Geneva,' 16 June 2021.

US Department of Justice. 'Emotet Botnet Disrupted in International Cyber Operation,' 28 January 2021. https://www.justice.gov/opa/pr/emotet-botnet-disrupted-international-cyber-operation.

US Department of Justice. 'Ukrainian Arrested and Charged with Ransomware Attack on Kaseya Office of Public Affairs,' 8 November 2021. https://www.justice.gov/archives/opa/pr/ukrainian-arrested-and-charged-ransomware-attack-keya.

US Department of Justice, 'US Department of Justice Disrupts Hive ransomware variant,' January 26, 2023,

https://www.justice.gov/archives/opa/pr/us-department-justice-disrupts-hive-ransomware-variant

US Department of Justice. 'Deputy Attorney General Lisa O. Monaco Delivers Remarks on the Disruption of Hive Ransomware Variant,' 26 January 2023. https://www.justice.gov/archives/opa/speech/deputy-attorney-general-lisa-omonaco-delivers-remarks-disruption-hive-ransomware-va.

US Department of Justice. 'US and UK Disrupt LockBit Ransomware Variant,' 20 February 2024. https://www.justice.gov/archives/opa/pr/us-and-uk-disrupt-lockbit-ransomware-variant.

US Department of Justice. 'Audit of the Department of Justice's Strategy to Combat and Respond to Ransomware Threat and Attacks,' September 2024. https://oig.justice.gov/sites/default/files/reports/24-107.pdf.

Virtual Routes. 'Ransomware Countermeasures Tracker.' Accessed 19 January 2026. https://virtual-routes.org/ransomware-countermeasures-tracker/.

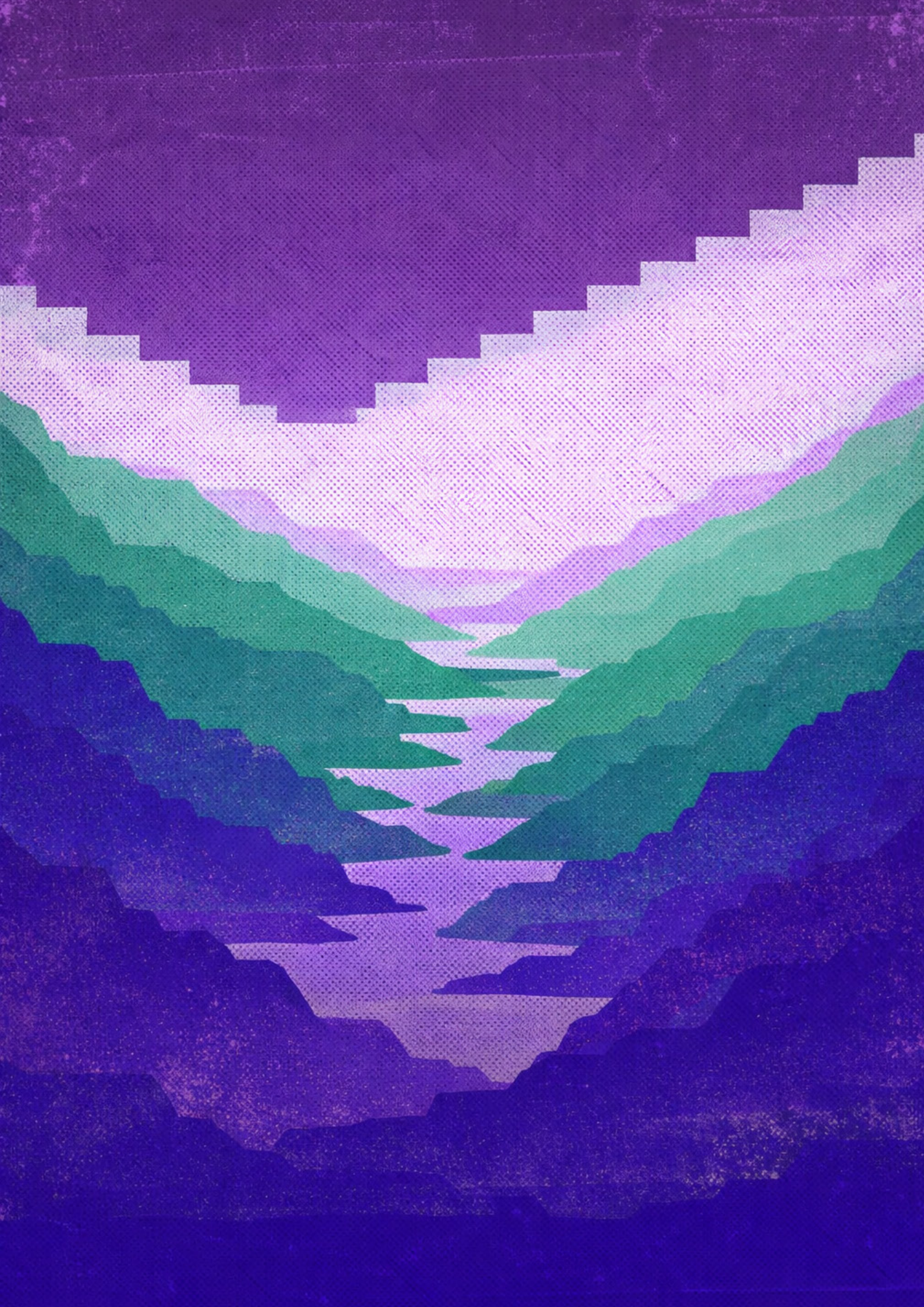
VX-underground. 'Interviewing the LockBit Administrator.' https://vxunderground.org/Papers/Other/Interviews/Interviewing%20the%20Lockbit%20Administrator.html.

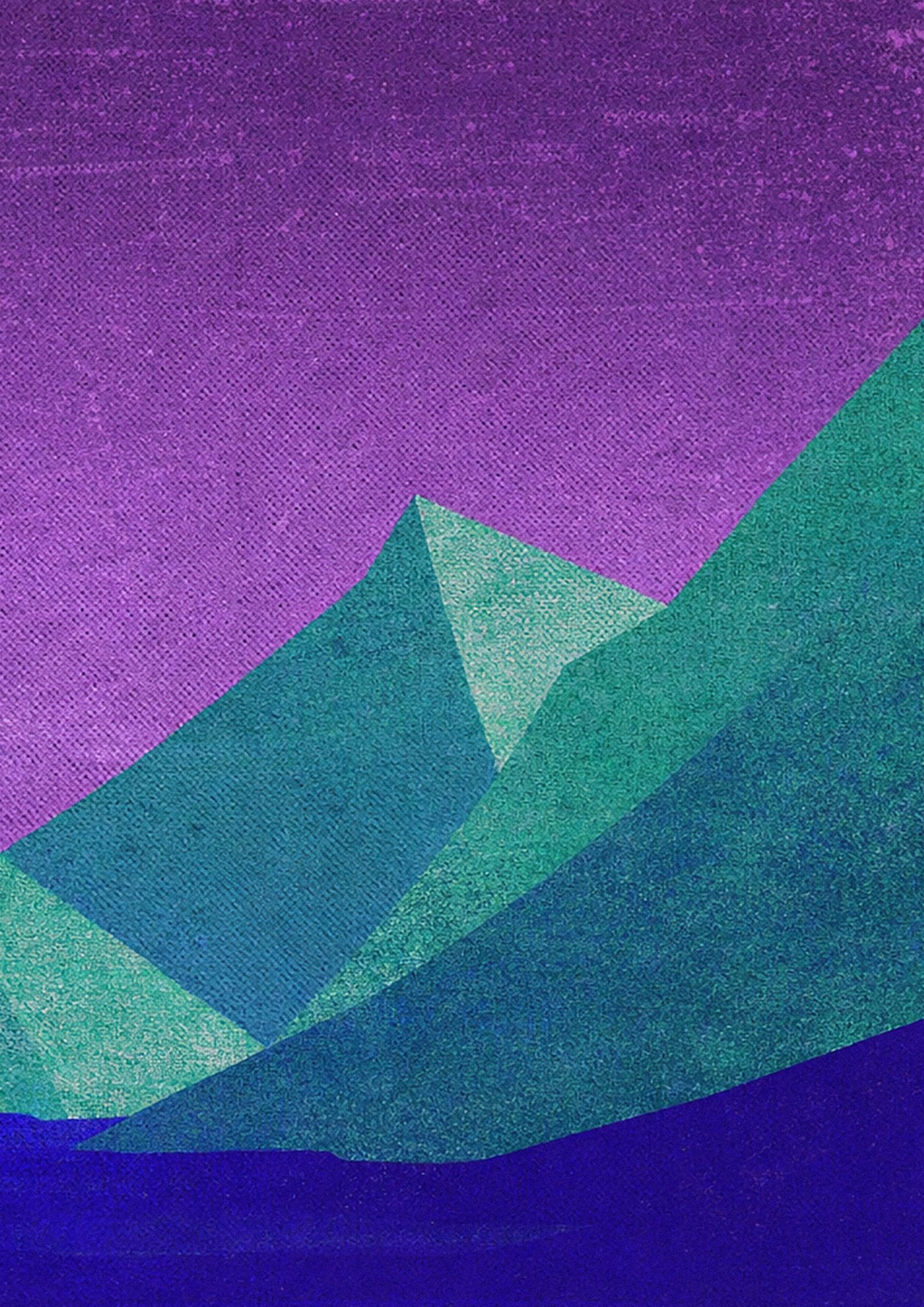
Waldman, Arielle. 'Distrust, Feuds Building among Ransomware Groups.' *TechTarget: Security*, 3 February 2022. https://www.techtarget.com/searchsecurity/news/252512902/Distrust-feuds-building-among-ransomware-groups.

Wray, Christopher, 'Remarks at press conference announcing the disruption of the Hive ransomware group,' January 26, 2023, https://www.fbi.gov/news/speeches-and-testimony/director-christopher-wrays-remarks-at-pressconference-announcing-the-disruption-of-the-hive-ransomware-group

Zohdy, Mahmoud, Pietro Albuquerque, and Abzal Aitoriyev. 'The Beginning of the End: The Story of Hunters International.' *Group-IB*, 2 April 2025. https://www.group-ib.com/blog/hunters-international-ransomware-group/.

Zugec, Martin. 'Hive Ransomware's Offspring: Hunters International Takes the Stage,' 9 November 2023. https://www.bitdefender.com/en-gb/blog/businessinsights/hive-ransomwares-offspring-hunters-international-takesthe-stage.





For more information, please visit: **www.virtual-routes.org**

If you have any further queries, questions, or concerns, feel free to reach out via email at:
contact@virtual-routes.org