

2023-09-22 08:05:22 VICTIM ID 8978

Hello, I am a IT specialist working with XXXX. You have locked our system and advised that I contact you here. Please advise how we can regain access to our data.

2023-09-22 08:05:22 VICTIM ID 8978  
We have been contacted by you. You pay us \$1.5 million. We will release your data. This is our 2023-09-22 VICTIM ID 8978. I will release your data. 2023-09-22 VICTIM ID 8978. I believe you

# EXERCISE VEIL STORM I

contact us. We provide link

## AFTER ACTION ANALYSIS

you need helps to get Bit-coin instructions.

an authority for such re-lease of data among management.

We are not here to waste time. You have 72 hours to us. If we do not hear from you, we will

begin to release your sensitive data. How you think that your customers going to like having their private and sensitive data leaked? Your reputation will be RUINED. Reputation worth \$1.5 million. This is small part of revenue. Tick Tock.

VICTIM 8987  
We do not want to upset you. It is just not possible for us to obtain approval from management and to arrange a payment of such a sum in such a short timeframe. If you give us a week, we could arrange for a payment of \$600,000.

2023-10-05 16:45:55 MANTICORE

We do not want to negotiate further with someone so stupid. If you are too lowly to make decision, you should not try. You must not care about your clients.

You are just greedy company who care more about money than customers. You are not interested in wasting time. YOU lose part data.

make  
ARE  
\$1.5  
2023-10-05

TAYLOR GROSSMAN

We  
series  
rang

JULY 2025

more of our data released. We are taking you very seriously. We will make a payment of \$1.5 million immediately. We could arrange for a payment of \$600,000 now and pay the rest under a separate payment.

2023-10-08 18:25:43  
MANTICORE

2023-09-22 08:05:22 VICTIM ID 8978

Hello, I am a IT specialist working with XXXX. You have looked our system and advised that I contact you here. Please advise how we can regain access to our data.

2023-09-22 14:32:45

MANTICORE

We are much pleased that you have made the good choice to contact us. We have your sensitive data (financial and customer information). We provide link below as proof.

You would be smart to meet our demands. We are not here to waste time. You pay, you get your files back. No games. Our interest here is to make money.

We have spend time in your network and study your revenues. You must pay \$1.5 million USD paid in bitcoin. If you pay in Monero, we are willing to provide you discount, \$1.4 million USD. For this price we will provide to you 1) tool to access your data 2) instructions on how to use tool to get your data and 3) provide you with information on your vulurabilities so you can patch system.

This is reasonable price. You have 72 hours to pay. If you need helps to get Bitcoin or Monero, let us know and we will provide for you instructions.

2023-09-25 09:10:07

VICTIM ID 8987

I will have to take this to the CEO as I do not have the authority for such requests. We will need more time to discuss among management.

2023-09-25 16:20:34

MANTICORE

I believe that we have been CLEAR. We are not here to waste time. You have 72 hours to talk to your CEO and get back to us. If we do not hear from you, we will begin to release your sensitive data. How you think that your customers going to like having their private and sensitive data leaked? Your reputation will be RUINED. Reputation worth \$1.5 million. This is small part of revenue. Tick Tock.

VICTIM 8987

We cannot possible for us to obtain approval from management and to arrange a payment of such a sum in such a short timeframe. If you gives a week, we could arrange for a payment of \$600,000.

2023-10-05 16:05:55 MANTICORE

We cannot work with someone so stupid. If you are too lazy to make decision, you should not try. You must not care about your clients. You are just greedy company who care more about money than customers. You make bad decision. We said from first, we not interested in wasting time. YOU ARE WASTING TIME. That costs. We will post part data.

\$1.5 million NOW.  
The Institute for Security and Technology and the authors of this report invite free use of the information within for educational purposes, requiring only that the reproduced material clearly cite the full source.

2023-10-06 07:34:23 VICTIM 8987

We do not want to have any more of our data released. We are taking you very seriously. We cannot arrange a payment of \$1.5 million immediately. We could arrange a payment of \$700,000 now and pay the rest under a separate payment.

2023-10-08 18:25:43

MANTICORE

Copyright 2025, The Institute for Security and Technology  
Printed in the United States of America

# About the Institute for Security and Technology

*Uniting technology and policy leaders to create actionable solutions to emerging security challenges*

Technology has the potential to unlock greater knowledge, enhance our collective capabilities, and create new opportunities for growth and innovation. However, insecure, negligent, or exploitative technological advancements can threaten global security and stability. Anticipating these issues and guiding the development of trustworthy technology is essential to preserve what we all value.

The Institute for Security and Technology (IST), the 501(c)(3) critical action think tank, stands at the forefront of this imperative, uniting policymakers, technology experts, and industry leaders to identify and translate discourse into impact. We take collaborative action to advance national security and global stability through technology built on trust, guiding businesses and governments with hands-on expertise, in-depth analysis, and a global network.

We work across three analytical pillars: the **Future of Digital Security**, examining the systemic security risks of societal dependence on digital technologies; **Geopolitics of Technology**, anticipating the positive and negative security effects of emerging, disruptive technologies on the international balance of power, within states, and between governments and industries; and **Innovation and Catastrophic Risk**, providing deep technical and analytical expertise on technology-derived existential threats to society.

Learn more: <https://securityandtechnology.org/>

# Acknowledgements

The Institute for Security and Technology (IST) organized and delivered this tabletop exercise and report in partnership with Europol's EC3. We are grateful for their support and for their willingness to host this exercise at their headquarters in The Hague.

IST would also like to acknowledge the team members from the UK National Crime Agency - National Cyber Crime Unit and the Royal Canadian Mounted Police National Cybercrime Coordination Centre that spearheaded the design and organization for Exercise VEIL STORM. We would also like to thank the many law enforcement officers, government officials, and private sector representatives that helped shape the tabletop. These individuals offered their time and invaluable expertise, and we could not have done this work without their insights and encouragement.

We would also like to thank the participants who joined us in The Hague for engaging fully with the exercise. Because of their enthusiasm, we are working to deliver Exercise VEIL STORM II in the fall of 2025.

Finally, the author would like to thank the many individuals who made this possible: the Ransomware Task Force International Engagement Working Group for pushing the exercise forward, and the expansive network of contributors to and supporters of the RTF, including Grupo Santander, Rick Scot, Megan Stifel, and Elizabeth Vish, who made this effort possible.



# Contents

- Overview .....1**
- Background..... 2**
- Exercise Design ..... 3**
  - Design Team..... 3
  - Participants and Tabletop Setup ..... 3
- Exercise VEIL STORM in Action ..... 4**
  - Objectives and Phased Structure..... 4
  - Phase 0: Meeting the Threat Actor ..... 5
    - Figure 1: Fictitious MantiCORE Ransomware Threat Assessment from the NC3 ..... 7*
    - Figure 2: Sample Fictitious TTPs.....9*
  - Phase 1: Cyber Incident Response ..... 9
    - Figure 3: Fictitious Victim Crime Reports..... 10*
  - Phase 2: Preparation for Payment ..... 14
    - Considerations for paying a ransom..... 14*
    - “Follow the money” ..... 16*
  - Phase 3: Payment Process and Beyond..... 18
    - Figure 4: Fictitious MantiCORE Seizure Page ..... 19*
- After Action Analysis ..... 20**
- Recommendations for Consideration..... 24**
  - 1. Clarify Existing Processes ..... 24
  - 2. Empower People ..... 24
  - 3. Create New Mechanisms ..... 25
- Conclusion and Next Steps ..... 27**
- Acronyms and Abbreviations ..... 28**

# Overview

Effective and timely information sharing is a crucial component to building operational collaboration across the public and private sectors, with the ultimate goal of mitigating cyber incidents and disrupting threat actors. In 2024, IBM found that ransomware victims who engaged with law enforcement reduced breach costs by nearly \$1 million USD on average. Even limited information sharing can help shorten breach lifecycles, reducing both costs and downtime for companies.<sup>1</sup> Private companies have also played crucial roles in recent law enforcement disruptions of cyber criminal groups, from alerting authorities about malicious activity to shutting down threat actor infrastructure.<sup>2</sup>

Through a partnership with Europol, the Institute for Security and Technology (IST) and the Ransomware Task Force's (RTF) International Engagement Working Group led the design and delivery of Exercise VEIL STORM, a tabletop exercise (TTX) focused on operational coordination across international law enforcement agencies and private sector firms in responding to cyber incidents. This report summarizes the proceedings and findings of that tabletop exercise, which took place at the Europol Headquarters in The Hague on the margins of the 2024 Europol Cybercrime Conference.

The Exercise VEIL STORM tabletop exercise generated valuable takeaways for enhancing operational collaboration and information sharing, as well as a series of recommendations for possible action:

## 1. Clarify Existing Processes

- a. Joint exercises can be leveraged to create more opportunities for organizations to work together.
- b. In an era of geopolitical uncertainty, bilateral and multilateral mechanisms for collaboration are more important than ever.

1 "Cost of a Data Breach Report 2024," IBM, August 2024, <https://www.ibm.com/downloads/documents/us-en/107a02e94948f4ec>.

2 There are several prominent examples of private sector actors participating in active law enforcement-led disruption campaigns in the past few years. In the 2020 Trickbot disruption, for example, Microsoft obtained a court order to shut down some of the group's infrastructure, while ESET and Lumen's Black Lotus Labs provided key intelligence about the group's TTPs. For more, see: Tom Burt, "New action to combat ransomware ahead of U.S. elections," Microsoft, October 12, 2020, <https://blogs.microsoft.com/on-the-issues/2020/10/12/trickbot-ransomware-cyberthreat-us-elections/>; Black Lotus Labs, "A Look Inside the TrickBot Botnet," Lumen, October 12, 2020, <https://blog.lumen.com/a-look-inside-the-trickbot-botnet/>. In the 2023 Qakbot takedown, the U.S. Department of Justice credited Zscaler with providing "valuable technical assistance" and Shadowserver, Microsoft, the National Cyber Forensics and Training Alliance, and Have I Been Pwnd for partnering "to aid in victim notification and remediation." For more, see: U.S. Attorney's Office, Central District of California, "Qakbot Malware Disrupted in International Cyber Takedown," press release, U.S. Department of Justice, August 29, 2023, <https://www.justice.gov/usao-cdca/pr/qakbot-malware-disrupted-international-cyber-takedown>.

## 2. Empower People

- a. Work to empower the proper emissaries for creating relationships between private companies and law enforcement.
- b. Build on existing efforts, such as the NCFTA, the RTF, ISACs, and the Cybercrime Atlas.

## 3. Create New Mechanisms

- a. Explore cyber insurance as a new lever to encourage information sharing.
- b. Examine the effects of sanctioning entities that facilitate money-launder operations on curtailing crime.
- c. Consider introducing private sector partners into international law enforcement operations to improve communication and build relationships.
- d. Create opportunities for private sector actors to develop close relationships with, and understanding of, law enforcement priorities and structures.
- e. Build a framework for ransomware disruption that allows for contributions from both law enforcement and private companies.

# Background

Information sharing and operational collaboration have long been focuses of IST and the RTF. In late 2020, IST launched the RTF, a multistakeholder effort with participation from across government, industry, and civil society, to identify and advance recommendations to reduce the risk of ransomware. Of the original 48 recommendations in the RTF's [Combating Ransomware](#) report ("the Report"),<sup>3</sup> nine targeted the ransomware information ecosystem, highlighting ways that financial industry entities, law enforcement agencies, and cyber incident response firms could work together to share information and coordinate activities to produce openings for strategic disruption. One key recommendation focuses on sharing information about ransomware payments in order to increase visibility and create opportunities for disruption across the full spectrum of a ransomware attack—from launch to laundering to resourcing—and ultimately weaken the capabilities of criminal and other malicious actors to profit from ransomware attacks.

In April 2024, the RTF published [Information Sharing in the Ransomware Payment Ecosystem – Exploring the Delta Between Best Practices and Existing Mechanisms](#),<sup>4</sup> which compared the findings from a ransomware attack scenario exercise conducted by the RTF with the

3 Ransomware Task Force, "Combating Ransomware: A Comprehensive Framework for Action," Institute for Security and Technology, April 2021, <https://securityandtechnology.org/ransomwaretaskforce/report/>.

4 Zoë Brammer, "Information Sharing in the Ransomware Payment Ecosystem: Exploring the Delta Between Best Practices and Existing Mechanisms," Institute for Security and Technology, April 2024, <https://securityandtechnology.org/virtual-library/reports/information-sharing-in-the-ransomware-payment-ecosystem/>.



results of recent collaborative operations, including the 2023 Hive takedown, the 2021 Emotet takedown, and the 2021 Colonial Pipeline disruption. The report highlighted key pressure points across the environment and recommended steps that the United States and its partner governments can take to bolster information sharing with the private sector to help scale existing best practices.

IST and the RTF partnered with Europol to design, execute, and analyze the results of Exercise VEIL STORM to further this work, informing our strategies as we continue taking action and pursuing research to deter and disrupt the ransomware ecosystem.

# Exercise Design

## Design Team

Europol and IST directed the exercise with facilitation support by a team consisting of members from the UK National Crime Agency - National Cyber Crime Unit (NCA/NCCU) and Canada's Royal Canadian Mounted Police National Cybercrime Coordination Centre (RCMP-NC3). The core design team included members from Canada's RCMP-NC3, Europol's European Cybercrime Centre (EC3) Policy and Development Team, IST, and the UK NCA/NCCU.

## Participants and Tabletop Setup

Exercise VEIL STORM took place at Europol Headquarters in The Hague on October 14, 2024. The exercise format was a tabletop exercise (TTX) and involved approximately five hours of exercise-related activity. Participants attended in person, with note-taking support from remote members of the IST and RCMP teams.

In close consultation with Europol, the design team selected participants from members of organizations across key nodes of the ransomware information ecosystem. Participants represented law enforcement agencies from the United States, Canada, Australia, and several European Union Member States (EU MS), EU MS-based prosecutors, and private industry—including financial institutions, cyber threat intelligence and analysis firms, incident response firms, and cryptocurrency exchanges. TTX organizers chose participants based on their knowledge and authority to represent their organization's processes and interests and speak on its behalf during the exercise discussions. Many participating individuals have held multiple roles within the cybersecurity community, including in the public and private sectors. Members of the Joint Cybercrime Action Taskforce (J-CAT) and European Cybercrime Centre (EC3) at



Europol also took part in the TTX and interfaced directly with the participants throughout the day.

# Exercise VEIL STORM in Action

## Objectives and Phased Structure

The overall exercise purpose was to “Identify and verify friction points within the ransomware payment ecosystem where an integration of effort, by key partners, could cause frustration for ransomware actors and contribute to meaningful cybercrime reductions.” The exercise objectives were as follows:

- » Given the current structure of European key component “service points” within the ransomware payment ecosystem and the current state of relationships and interactions, identify what critical information requirements organizations have that could be augmented by improvements in communication and collaboration.
- » Understand where, within the system of engagements active during a cyber incident response, “pinch points” exist where information is not shared that could potentially reduce further risk to victims or cause potential points of friction for ransomware bad actors.
- » Focusing on the points within the ransomware cyber incident response process relating to payments and the associated key points of interaction between all those engaged, identify points where improved integration of effort or the introduction of other key cybercrime reduction partners could reduce ransomware associated risks.
- » Identify—based on the policy, legal and operational frameworks currently informing the activities of organizations involved within the functioning processes of the ransomware ecosystem—where opportunities exist to improve connectivity, information sharing channels, or tactical and operational integration of efforts to create viable friction for ransomware bad actors.
- » Improve the understanding of current law enforcement activities to disrupt the ransomware payment ecosystem and identify potential to improve collaboration and integration of effort through greater transparency with external partners who have a shared interest in cybercrime reduction.

The TTX consisted of a pre-briefing and level-setting discussion followed by three phases: (1) Cyber Incident Response, (2) Preparation for Payment, and (3) Payment Process and Beyond. Across these phases, the organizers introduced seven tailored injects, focusing on key pinch

points across the international ransomware payment ecosystem. The exercise explored key entities in the negotiation and payment process, their respective roles and responsibilities, and opportunities and challenges related to information sharing over the course of an incident.

The design team made a deliberate choice not to assign a participant to play the role of the ransomware victim or the ransomware attacker. Instead, participants spoke from their own experiences as members of their current or former organizations. The design team facilitators provided inject materials to facilitate discussion and explain actions taken by the victim(s) and the attacker(s).

## Phase 0: Meeting the Threat Actor

Prior to the start of Operation VEIL STORM, participants read a pre-briefing handbook outlining the scenario. This handbook included information about a fictitious threat actor named MantiCORE Group, a ransomware gang first observed in spring 2023 and known to engage in triple extortion.<sup>5</sup> Based on threat intelligence from NC3, the group is believed to be based in Russia or another country in the Commonwealth of Independent States (CIS). The group “has gained the attention of international law enforcement due to its aggressive extortion tactics, targeting of critical infrastructure and supply chain attacks,” and has targeted at least 103 victims internationally.<sup>6</sup> While the group was first active in North America, it has since moved its focus to Australia and Western Europe. Threat intelligence provided to participants also included information on the group’s tactics, techniques, and procedures (TTPs), highlighting MantiCORE’s exfiltration styles and negotiation tactics. The report also mapped observed behavior to the MITRE ATT&CK framework.<sup>7</sup>

At the start of the formal exercise, participants discussed the briefing package and the nature of the threat actor. Participants noted that the threat actor had been specifically focusing on managed service providers (MSPs), which can often be harder to defend once they have been infiltrated by an attacker. A ransomware actor can take over control of the MSP dashboard, thus gaining the ability to run commands in the target environment, including associated businesses that use the MSP.

Participants reflected on the importance of understanding the general structure of the threat actor, particularly whether the actor operates as a core ransomware group or as a Ransomware-as-a-Service (RaaS) group.

---

5 Triple extortion occurs in three phases: (1) a ransomware group demands a ransom for access to a decryptor after encrypting victim data; (2) the ransomware group exfiltrates victim data and threatens to leak it unless a ransom is paid; and (3) the ransomware group threatens to contact the victim’s clientele or customer base if a third ransom is not paid.

6 *VEIL STORM Player Handbook* (The Hague: Institute for Security and Technology and EUROPOL EC3, 2024), p. 12.

7 “MITRE ATT&CK®,” last accessed June 2025, <https://attack.mitre.org/>.

A core ransomware group is a smaller group that generally runs ransomware operations independently. These groups usually conduct their own initial access operations, deploy their own engineered ransomware strains, and launder their ransom payments. A core ransomware group maintains full control over the operation in a “closed loop.”

A RaaS provider is a malicious iteration of the traditional Software-as-a-Service (SaaS) model, whereby one party develops software and sells it to others for use. Here, the RaaS organization builds a strain of ransomware and the tools to deploy it and sells its wares to interested buyers.<sup>8</sup> RaaS entities can even rent infrastructure and other services for launching an attack, making it easy for a buyer, or affiliate, to deploy ransomware. RaaS providers deal with many affiliates who use varying TTPs; affiliates may also target different types of victim entities (perhaps a certain kind of company, like an MSP, or companies that operate out of a specific region) based on where they can gain the most access. Affiliates may purchase access through brokers or create their own entry points into victim networks.

Understanding whether a threat actor operates primarily as an independent organization or through affiliates can help responders map out how that actor will process payments, launder money, and facilitate operations across different jurisdictions.

---

8 “What is Ransomware as a Service (RaaS)?,” Palo Alto Networks, last accessed June 2025, <https://www.paloaltonetworks.com/cyberpedia/what-is-ransomware-as-a-service>.

**EXERCISE EXERCISE EXERCISE**

*This document is marked as **FOR TRAINING PURPOSES ONLY**  
This document has been produced for the purpose of a training exercise only  
and does not contain true data.*

## MantiCORE RANSOMWARE

### QUICK FACTS

The aim of this report is to provide an overview of the MantiCORE ransomware group. MantiCORE was first observed in March 2023. The MantiCORE ransomware group has been known to engage in triple extortion<sup>1</sup>.

In 2023, the NC3 observed 11 cases involving BianLian ransomware. This variant was previously assessed through the NC3's Top Ten Ransomware Variants Impacting Canada at number eight in the quarterly period from May to August 2023.

**LEAK SITE URL:** [http://manticorekajshdfkjljsahfkljsdhflkjashdlkjfhakljsdadfdsafd\[.\]onion](http://manticorekajshdfkjljsahfkljsdhflkjashdlkjfhakljsdadfdsafd[.]onion)

**FIRST OBSERVED IN WILD**

March 2023

**LAST ACTIVE ON DARKWEB**

2024-10-09

**SUSPECTIVE MOTIVE**

Financial

**SECTOR MOST TARGETTED**

IT & Communication Technology, Energy, Supply Chain

**DISTRIBUTION METHOD**

Remote Desk Protocol credentials

**CANADIAN VICTIMIZATION**

13 known Canadian victims

**ENCRYPTED FILES EXTENSION**

".manti"

**RANSOM NOTE TITLE/FORMAT**

MantiCORE\_readme.txt

**SHADOW COPIES DELETION**

Yes

**ENCRYPTION TOOL**

AES-256, ChaCha20

Figure 1: Fictitious MantiCORE Ransomware Threat Assessment from the NC3<sup>9</sup>

9 VEIL STORM Player Handbook (The Hague: Institute for Security and Technology and EUROPOL EC3, 2024), p. 11.

Attendees noted that MantiCORE appeared to be a smaller ransomware group working without extensive affiliates. Instead, the threat actor uses a strong, centralized structure and strategically shifts between geographic targets, helping them avoid detection. Through jurisdiction hopping, the group has been able to evade garnering too much attention from one set of law enforcement authorities.

TTX participants also observed that MantiCORE employs a sophisticated payment strategy. The group offers victims the option to pay in Bitcoin at full price, or an alternate privacy-based cryptocurrency such as Monero at a discount. This suggests that the group understands Bitcoin's traceability and the risks associated with possible identification, and thus adjusts its operations to better launder funds and avoid detection.

Attendees discussed MantiCORE's triple extortion procedure, which suggests a focus on targeting a company's reputation as well as its financial and operational security. In the read-ahead material, past victims provided testimony citing MantiCORE's aggressive tactics as the primary motivation for engaging in negotiation and eventual ransom payment.<sup>10</sup>

Participants observed that triple extortion remains a relatively rare model for ransomware groups. LockBit and Scattered Spider (also known as Octo Tempest), for example, have been observed using triple extortion, where the groups target individuals with specific threats such as DDoS attacks, physical intimidation, or violence.<sup>11</sup> However, most major ransomware gangs have gravitated toward double extortion: first, they encrypt a victim's data and demand a ransom for the data to be decrypted; second, they threaten to release copied private or sensitive data onto the dark web unless an additional ransom is paid. By threatening to target clients and customers directly, including through threats of DDoS attacks and other mechanisms of triple extortion, the participants deduced that MantiCORE focuses on dominating and isolating the victim as much as possible from the outset.

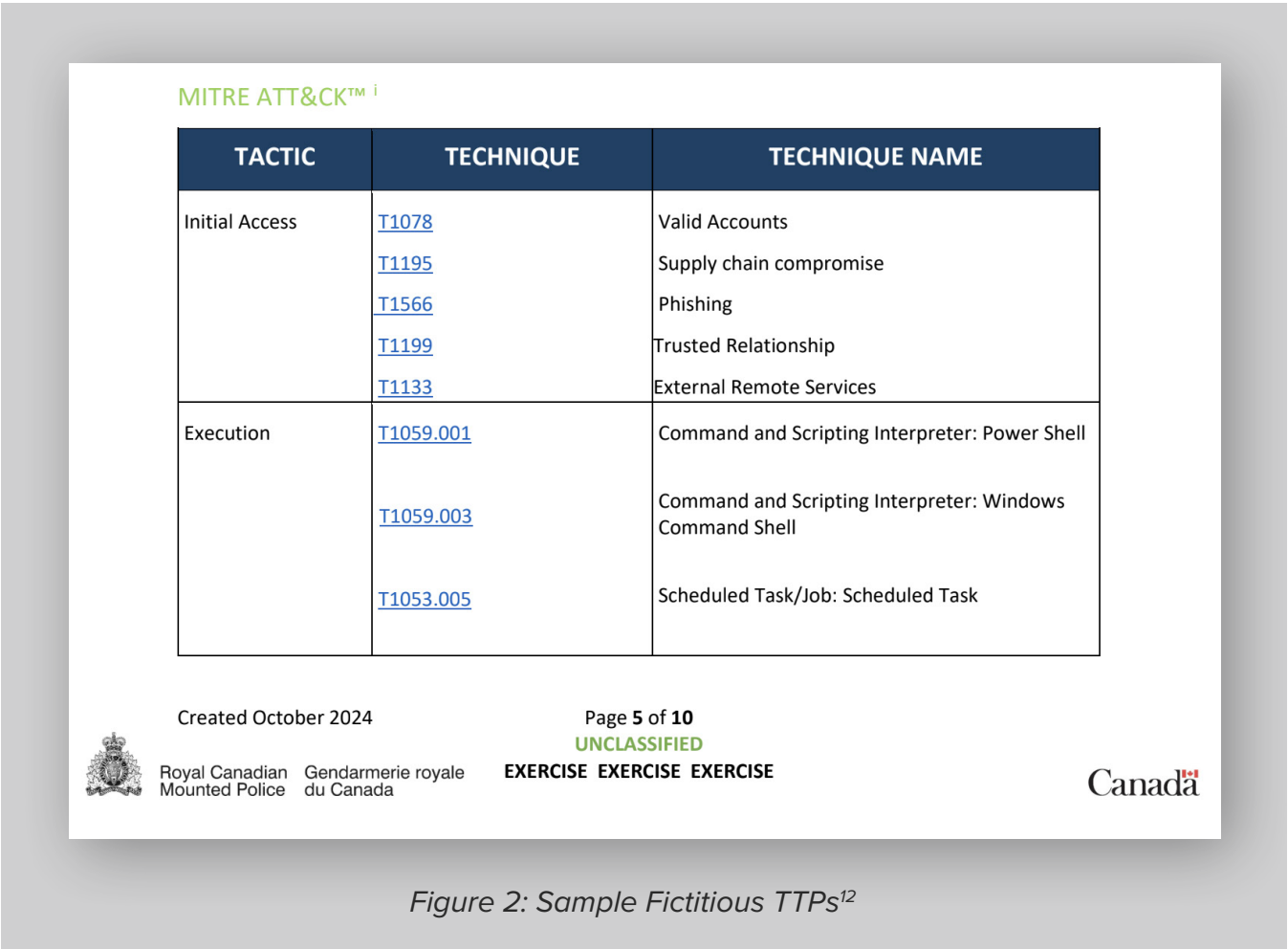
Finally, attendees noted the utility of being provided extensive background information on the threat actor, including known TTPs mapped onto a shared vocabulary and framework like the MITRE ATT&CK typology. Private sector participants noted that this kind of information can help their organizations engage with their own third party vendors to attempt to assess ecosystem-level risk and align controls to get ahead of an ongoing incident. As became

---

10 "Setting the Scene: Exercise Veil Storm Story Line & Context" in *VEIL STORM Player Handbook* (The Hague: Institute for Security and Technology and EUROPOL EC3, 2024), p. 1-3.

11 See, for example: Nathan Eddy, "Octo Tempest Group Threatens Physical Violence as Social Engineering Tactic," *DarkReading*, October 27, 2023, <https://www.darkreading.com/threat-intelligence/octo-tempest-group-threatens-physical-violence-social-engineering-tactic/>; Ionut Ilascu, "LockBit ransomware gang gets aggressive with triple-extortion tactic," *Bleeping Computer*, August 28, 2022, <https://www.bleepingcomputer.com/news/security/lockbit-ransomware-gang-gets-aggressive-with-triple-extortion-tactic/>. One participant also noted cases of a ransomware actor threatening to alert a victim's regulators of the ongoing incident and data breach to try and bully the organization into paying ransoms.

clear in later discussions, participants agreed that if notified of such an incident, they would immediately work to assess their own exposure to a sophisticated actor like MantiCORE.



# Phase 1: Cyber Incident Response

Facilitators introduced participants to three fictitious organizations who had just suffered a fictitious ransomware attack:

- 1. Krystel Financial Services, a company founded and based in the Netherlands that offers “Buy Now, Pay Later” (BNPL) services.**
  - » BNPL allows consumers to make purchases and pay them in installments, either in four interest-free payments or within 30 days. Krystel also has offices across France, the United Kingdom, Germany, Australia, Canada, and the United States.

<sup>12</sup> VEIL STORM Player Handbook (The Hague: Institute for Security and Technology and EUROPOL EC3, 2024), p. 5.



**2. ClientWave, a company headquartered in the United Kingdom that performs customer service roles for Krystel.**

» ClientWave is a leader in the customer service industry, aiming to simplify interactions and enhance customer satisfaction. The company also has offices across Europe including France, Germany, and the Netherlands.

**3. NextGen Solutions, a company headquartered in the United States that performs financial crime prevention and operational support roles to Krystel.**

» NextGen Solutions is a global professional services company specializing in consulting and technology services. The company has over 700,000 employees with offices across the United States, Canada, Australia, and Europe.

As the tabletop exercise began Phase 1, participants learned that Krystel Financial services was the first to be hit by a ransomware attack, which led to a shutdown of their operations globally, including their offices across Europe in the Netherlands, France, England, and Germany. The attack also spread to their partners, ClientWave and NextGen Solutions. Krystel's headquarters in Amsterdam and Paris and ClientWave's headquarters in London reported the incidents to law enforcement and their national CERTs. However, American partner NextGen Solutions has yet to make a report to its law enforcement and cybersecurity authorities, including the FBI and CISA.




<p><b>Victim Crime Report</b> </p> <p>Victim: Krystel Financial Services (Dutch Based Company with offices across the globe).</p> <p>Incident details:</p> <ul style="list-style-type: none"><li>• Ransomware attack perpetrated by the MantiCORE Ransom Group, which has resulted in the complete shutdown of operations spreading across all their international offices. The shared portal utilised to work with their partners ClientWave and NexGen Solutions has also been affected.</li><li>• A CIR company has been deployed.</li><li>• Ransomware note left demanding €20,000,000 to be paid in bitcoin within 96 hours.</li><li>• In the note they have claimed to have infiltrated their network and encrypted all critical data.</li><li>• No decision has been reached to pay the ransom yet. The business remains fully non-operational across all international offices.</li></ul>	<p><b>Victim Crime Report</b> </p> <p>Victim: Krystel Financial Services (Dutch Based Company, Report made by secondary headquarters in Paris).</p> <p>Incident details:</p> <ul style="list-style-type: none"><li>• Ransomware attack perpetrated by the MantiCORE Ransom Group, which has resulted in the complete shutdown of operations spreading across all their international offices. The headquarters in Paris has been severely impacted.</li><li>• A CIR company has been deployed.</li><li>• Ransomware note left demanding €20,000,000 to be paid in bitcoin within 96 hours.</li><li>• In the note they have claimed to have infiltrated their network and encrypted all critical data.</li><li>• No decision has been reached to pay the ransom yet. The business remains fully non-operational across all international offices.</li></ul>	<p><b>Victim Crime Report</b> </p> <p>Victim: ClientWave Customer Service Provider (UK based company with offices across Europe).</p> <p>Incident details:</p> <ul style="list-style-type: none"><li>• Ransomware attack by the MantiCORE Ransom Group, stemming from a prior breach to Krystel.</li><li>• The attackers infiltrated Krystel's systems and leveraged this access to compromise ClientWaves network, resulting in the complete shutdown of operations.</li><li>• A CIR company has been deployed.</li><li>• Ransomware note left demanding £8,000,000 to be paid in bitcoin within 96 hours.</li><li>• In the note they have claimed to have infiltrated their network and encrypted all critical data..</li><li>• No decision has been reached to pay the ransom yet. The business remains fully non-operational across all European offices.</li></ul>
--	--	--

Figure 3: Fictitious Victim Crime Reports<sup>13</sup>

<sup>13</sup> Operation VEIL STORM, powerpoint, Institute for Security and Technology and EUROPOL EC3, 2024, slide 12.



Facilitators asked participants to share perspectives on their organization and/or sector's current level of situational awareness about an evolving ransomware threat such as that posed by MantiCORE. Discussion revolved around facilitator questions such as: How would law enforcement respond to these incidents? How would national law enforcement agencies decide whether to involve Europol?

Participants immediately honed in on the complications ensuing from the fact that the ransomware attack affected multiple jurisdictions. Some law enforcement faces key questions about where to report and which organization holds primacy over an evolving situation. One participant asked how a lead agency is determined. Law enforcement attendees noted that there is no one answer—a primary point of operations is determined through a combination of evaluating strengths and weaknesses of the jurisdictions involved and optimizing for potential to manage risk and achieve successful outcomes (such as fund seizures or arrests, if possible).

Other attendees disagreed, arguing that the primary jurisdiction will be determined based on where the headquarters of a company is located. However, victims could be located across multiple jurisdictions, which could further complicate the response efforts.

As the scenario progresses, because the incident has become public, companies that are not directly involved in the incident response phase, such as financial services firms, are also likely to launch internal procedures to check whether their providers might be involved. Organizations may begin to take protective actions, like limiting communications or restricting emails, in order to prevent the company from becoming infected by the same threat. Participants noted that private companies will immediately consider containment options and evaluate whether they have clients or suppliers and providers affected by the ongoing incident.

Since Krystel is a financial services company, participants agreed that information sharing mechanisms across the private sector will be robust and quickly activated. Attendees noted that the victim would be likely to reach out through official and unofficial channels to quickly gather details on attack vectors and indicators of compromise (IOCs). This process will almost certainly involve contacting the sector-specific Information Sharing and Analysis Center, FS-ISAC, as well as using more informal channels to connect with industry colleagues. Krystel will want to gain relevant details as soon as possible to protect themselves, and other companies in the industry will follow suit. Participants noticed that the financial sector differs somewhat from other sectors in the sophistication and maturity of its information-sharing mechanisms. Because it is so heavily regulated, financial services work closely with the FS-ISAC and other collaborative institutions like the Cyber Defence Alliance.<sup>14</sup>

---

<sup>14</sup> The Cyber Defence Alliance is a UK-based cyber threat intelligence organization composed of a number of banks and law enforcement agencies. See: "Homepage," Cyber Defence Alliance, last accessed June 2025, <https://cyberdefencealliance.org/>.

Meanwhile, cloud service providers (CSPs) would also be carefully watching this situation unfold, as such a major ransomware attack could have an impact on their own platform's users. If a platform vulnerability contributed to the incident, for example, CSPs would need to decide whether to notify their customers. However, participants also highlighted the challenge of balancing customer privacy, law enforcement involvement, and their responsibility to protect their users, which can complicate any decisions regarding notification or collaboration with governments.

Industry participants noted that a company's primary concern will be incident response: containing the crisis as quickly as possible, reassuring affected clients or consumers, and remediating the issue so they can resume normal operations. Although victim organizations want to catch the culprits, sharing information with law enforcement may not be a central concern in the immediate chaos of an unfolding incident. In the financial sector, companies face more stringent regulations and may be required to work more quickly to report an incident with relevant regulators and authorities. However, information sharing may still take days, not hours.

Industry participants also noted that they often do not know whether or to what extent law enforcement is already tracking a particular threat actor. This information could be useful in guiding internal decisions about where to go with information. Law enforcement attendees explained that there is a process for agencies operating in different jurisdictions: when a significant incident is reported—either directly or through local police—national authorities coordinate and then reach out to Europol to determine if there is already an operation underway. Sometimes, this coordination happens at the national level.

Europol's Secure Information Exchange Network Application (SIENA) acts as a valuable resource in the early stages of a major ransomware incident. As a first step, law enforcement agencies—including non-EU MS such as those in the United States, Canada, and Australia—ensure that any incidents are shared through SIENA.<sup>15</sup> Through the EC3's Cyber Intelligence Gateway (CIG), Europol can act as a hub or single entry door for obtaining information from third parties and the private sector, which helps bolster ongoing investigations.

As the scenario progressed, attendees discussed the immediate difference in priorities between law enforcement and incident response that emerges in an ongoing case. Agencies wishing to eventually build a case around a particular incident may be inclined to slow down or discourage information sharing because of important concerns around preserving a clear chain of evidence, as well as possible issues that could arise with personally identifiable information (PII) and other regulated data being shared in violation of existing regulations (such

---

<sup>15</sup> More than 3,500 authorities connect to SIENA, including EU member states and third countries which have cooperative working agreements with Europol.

as the EU's General Data Protection Regulation, or GDPR). Incident responders, meanwhile, will be focused on doing everything possible to stop or mitigate an attack as it unfolds; they are naturally less concerned with building a legal case against the perpetrators down the road, and are instead fighting to reduce immediate harms. This may incentivize practical moves that do not prioritize or secure evidentiary claims and instead maximize short-term impact to reduce the harms faced by victims.

Law enforcement agencies in particular face the challenge of how to balance competing priorities in ongoing incidents. Law enforcement is inclined to work toward dismantling criminal operations, but they also want to protect and secure victims. Some participants noted that many law enforcement agencies have engaged in community outreach in order to persuade organizations that they can provide immediate relief in an unfolding attack situation and will not seek to halt necessary incident response procedures. However, many misconceptions persist among victim (or potential victim) organizations. At the same time, not all law enforcement agencies—or even branches of the same agency—operate in the same way. Building relationships across law enforcement agencies and private companies is crucial to creating an optimal environment for incident response that also can benefit longer-term strategic disruption operations.

The scenario made clear that there is not a one-size-fits-all solution to incident response: each case may necessitate a slightly different response plan based on the unique challenges faced by the victim organization. However, law enforcement can benefit from having a better understanding of the myriad challenges that organizations face when confronted with an ongoing cyber incident, and from harmonizing responses.

Participants discussed ways to promote community engagement before incidents occur, including through more routine interactions between law enforcement agencies and the organizations in the communities that they serve. Several participants shared success stories related to increased investment in community engagement: as an important first step, law enforcement and industry interact through normal day-to-day operations, which can lead to the kinds of trusted relationships that are essential in the midst of an unfolding crisis. If introductions only occur during an incident, it may be too late to build lasting trust between these communities. Participants noted that confidence building measures like tabletop exercises and town halls can facilitate better proactive community relationships that can be leveraged if and when a crisis occurs.

# Phase 2: Preparation for Payment

In the second phase, facilitators asked participants to consider the necessary steps their organizations would take as a victim organization preparing to make a ransom payment. Since the facilitators—and not any one participant—played the role of the victim, the scenario focused on presenting attendees with a ransomed organization that had decided to pay the ransomware actors and understanding what comes next.

Krystel and ClientWave decided to pay the ransom due to the status of their backup restoration and new threats from MantiCORE. Both companies thus began taking steps to enter negotiations with the threat actors.

## Considerations for paying a ransom

Victim organizations face an immediate question regarding whether to pay a ransom. Ransomware gangs usually first approach victims with a single-extortion demand: pay a ransom to get your data returned and decrypted, so you can resume regular business operations. Many ransomware gangs continue to promise that they will delete victim data once this first demand is met.

Most incident response firms and law enforcement agencies know that this is often a false promise: ransomware actors frequently do not in fact erase data once it has been exfiltrated and encrypted in a ransomware attack. Victims, however, do not always know that this is the case. Thus, many organizations that have been hit by a ransomware attack do not realize that they will likely face a second, double-extortion attack; if they pay for their data to be decrypted, they will then face another threat to pay a ransom or suffer sensitive data being leaked online. Scenario participants noted that victims should be made aware as early as possible that their data has been copied and will be held by ransomware actors, and that they should keep this in mind when considering any form of payment.

During phase two of the scenario, victims also weigh regulatory concerns around leaked information. In Europe, GDPR regulations mean that a company can face serious fines if they suffer a breach of PII. Respondents disagreed on whether cooperating with law enforcement could help reduce or remove fines or regulatory consequences. Any leeway given to victims for reporting on and assisting with an investigation is usually kept confidential, as publicizing such information could cause unintended consequences for the victim or compromise the integrity of an ongoing investigation. It is thus difficult to say beyond anecdotal evidence whether cooperation with law enforcement can mitigate regulatory consequences down the road.

Several attendees also recognized that victims face subtler, psychological costs in paying or not paying a ransom. Even if a targeted organization recognizes that its data has been copied and that they may face double-extortion threats later on, they may be reluctant to see their logo up on a ransomware actor's website as an entity that has been successfully attacked. Some ransomware actors promise to withhold publicity around a breach on their leak sites. Even though the incident may become public in other venues, there can be comfort in not having an organization mentioned directly on a ransomware actor's own websites. This kind of cost, while harder to rationally justify, often comes into play when a victim considers the benefits and potential ramifications of paying a ransom.

Participants agreed that while these phases of an incident are often portrayed as discrete events, in reality they happen simultaneously: victims often discover they have been hit by a ransomware incident when they receive a payment demand, and have to determine how they plan to respond under enormous time pressure. Attackers capitalize on a victim's sense of isolation. A victim often must work to engage its incident response firm at the same time as it responds to its attacker. Sometimes, negotiating can be a useful tactic to buy time, allowing a victim to evaluate its exposure and bring in external experts while it deals with the ransomware actor.

Participants considered the views of incident response firms and law enforcement agencies as well. Most agreed that victim organizations will be counseled against involving law enforcement, particularly by lawyers concerned with unknown ramifications of sharing sensitive information and potentially losing direct control over decisions of how to interact with the threat actor. Facilitating better relationships between victims, incident response firms, and law enforcement is crucial to creating better information sharing and operational collaboration during incidents.

Many victim organizations view a ransomware attack as an internal failure and worry about the costs to their reputation if they proactively report to and engage with the authorities. While some companies may view collaboration with law enforcement as a boon to their reputations, others fear that it will impede consumer trust and damage their credibility in the broader market. Victims may not be aware of what law enforcement agencies can do to help mitigate an incident and aid injured parties. Some participants noted that law enforcement agencies need to do more to demonstrate their value to victims beyond targeting and catching perpetrators. However, many participants agreed that even when law enforcement does showcase the ways it can assist victims in the midst of an ongoing crisis, biases persist, and organizations may still opt to go it alone rather than collaborate at the outset.

Ultimately, participants agreed that deciding whether or not to pay a ransom depended on a number of internal factors, including the victim's organizational policies and crisis response

structures, and external factors, such as its specific regulatory environment. Participants agreed that tabletop exercises and other similar venues provide valuable opportunities to share and consider different perspectives related to these risk factors. Through these relationship-building discussions, law enforcement can better understand how a company weighs its options in the midst of an incident and where more community engagement and education could be helpful in demonstrating how law enforcement agencies might assist in these crises.

Participants also noted that in some cases, third parties may be a better advocate for involving law enforcement than field agents themselves. Attendees noted that incident responders, cyber insurers, and other external experts could help make the case for involving law enforcement authorities earlier in the process and could even help incentivize cooperation by building engagement into their plans and policies.

### **“Follow the money”**

In the TTX scenario, because the victim organization is a financial institution, it faces heavy regulation and is required to file suspicious activity reports (SARs) in many jurisdictions. Attendees noted that victims in this space are much more accustomed to reporting to various regulatory bodies and will certainly factor in these existing reporting guidelines as they approach paying a ransom demand. This makes financial institutions distinct from other types of ransomware victims, who may not have as clearly defined regulatory responsibilities.

Participants noted that many entities involved in incident response and payment platforms face degrees of risk when working with a victim organization as they prepare to pay a ransomware actor. For example, many cryptocurrency exchanges recognize that they take on a certain amount of risk when they facilitate ransom payments, as they could be engaging with sanctioned entities or other suspect organizations.

Cryptocurrency exchanges and payment platforms also retain key visibilities into the broader ransomware payment ecosystem and have unique opportunities to “follow the money” and shed light on ransomware gang behavior and infrastructure. More sophisticated payment platforms have noted that this visibility does more than create a reactive posture—helping them track a payment as it is being made by a victim to a ransomware gang. In addition, some companies can also use it to create a proactive posture, enabling them to see broader money laundering patterns and gather information that could help law enforcement strategically disrupt cyber-criminal networks before an attack occurs. Cryptocurrency exchanges could also have the ability to block incoming funds and/or freeze the funds already in the wallets.

Other private sector entities involved in the payment process can start to identify infrastructure being used by malicious actors to launch criminal attacks. For example, crypto exchanges

and blockchain firms can watch for transactions involving wallets known to engage in illegal activity. These entities have opportunities to flag suspicious behavior and share that information with law enforcement in real time. Payment platforms can watch for irregular consolidation of funds, which is often an indicator of illicit activity.

However, victim organizations worry about the downsides of sharing information with law enforcement agencies. Victims worry about the possible blowback they may face if ransomware gangs notice that they are collaborating with law enforcement agencies. In fact, many victims are explicit about not wanting to get their money back through law enforcement action because they fear further revictimization from ransomware actors. In some cases, victims have a strong incentive not to share specific wallet information with law enforcement because they are concerned about retaliation.

During phase two of the scenario, participants disagreed about whether creating friction in the payment ecosystem before a victim pays acts as a useful tool for reducing the profitability of ransomware. Some argued that victims who are set on paying cannot be usefully dissuaded and that attempts to slow down payment only create more opportunities for ransomware actors to further extort victims. Others instead contended that the more due diligence and compliance steps introduced into the payment process, the more likely a victim will rethink their decision to pay a ransomware actor as they contemplate the many possible regulatory, legal, and reputational consequences they may face. Much of this discussion is predicated on participants' opinions on current sanction regimes and whether or not sanctions issued by the U.S. Office of Foreign Assets Control (OFAC) and the UK Office of Financial Sanctions Implementation (OFSI) effectively deter criminals and victims alike.

Attendees noted that incident response firms, payment platforms, and other non-governmental actors can balance victim concerns of retaliation while also aiding broader law enforcement efforts to shut down and disrupt cyber criminal networks. Organizations can flag suspicious activity, including irregular cash flows. Meanwhile, analysts can observe how money moves along the blockchain, identifying patterns of cash outs that can help indicate possible affiliates and reinvestment schemes as major players resource their operating infrastructure. These entities can begin to map how a ransomware gang is operating internally and report on these broader behaviors to law enforcement without involving an individual victim.

Participants also discussed the practical utility of privacy-based cryptocurrencies like Monero in comparison to more mainstream cryptocurrencies like Bitcoin. While some ransomware gangs offer ransom discounts if a victim pays using a more private currency like Monero, the gangs may not actually stand to benefit significantly from using these more obfuscated currencies. Some participants pointed out that Monero and other such currencies do not have as broad or diversified a market as a currency like Bitcoin, and so a major ransomware



payment is much more likely to shift the market in a way that is noticeable to outside observers. While such a payment does not leave clear indicators on a crypto ledger, it is still observable because it will make serious waves in the marketplace. Other attendees had different points of view, arguing that when cybercriminals use Monero and other privacy-based cryptocurrencies, they make things more difficult for law enforcement to track and disrupt illicit activity.

Some participants noted that because the market for cybercrime has become so large, less cryptocurrency has to be laundered back into fiat currency (government-issued, non-crypto money). As a result, cryptocurrency stays in the system, and major cybercrime gangs can use it as they resource future operations, reinvesting funds back into the ecosystem to acquire tools and services that can help them continue to carry out attacks. Thus, the cash out process has become more nuanced. A \$2 million ransom crypto payment will not necessarily translate directly into a \$2 million fiat cash out; a non-trivial portion of this money will instead stay in cryptocurrencies.

Cryptocurrency exchanges can often see these developing patterns but may not be able to share this information with one another due to regulatory constraints—either real or perceived. Some exchanges worry about running afoul of GDPR or other privacy regulations, while others fear backlash for facilitating transactions that are eventually identified as illicit. Exchanges also face steep competition: there are plenty of crypto exchanges and mixers that do not practice any due diligence, and thus entities that want to comply with legal and regulatory regimes face serious business repercussions. Their customers will simply go to an exchange that conducts less scrutiny and due diligence of transactions.

Participants agreed that increased cross-sector collaboration among key industries within the payments space could help improve visibility. Broader inclusion of stakeholders is also important, as entities within the crypto industry may shift their policies and practices over time. Some institutions gain reputations for poor know your customer (KYC) or anti-money laundering (AML) practices but may become more compliant later on for a variety of factors, including a desire to become more legitimized or to attract new clients and engage in new regions. Participants noted that the broader community needs to work to create pathways for organizations to develop better compliance practices and to facilitate building back trust.

## Phase 3: Payment Process and Beyond

As the scenario exercise moved to phase three, facilitators informed participants that the victim successfully executed a ransom payment, the cyber incident response company received the decryption tools from the attackers, and incident responders have begun analyzing the tools for any hidden issues. Facilitators also told participants that the victim

notified law enforcement of the transaction, prompting law enforcement to begin monitoring the cryptocurrency exchange for any suspicious activity or attempts to trace the funds.

Working together, the crypto exchanges and law enforcement agencies successfully tracked the movement of the ransom payment and were able to identify where a portion of the payment eventually went.

This engagement led to a significant boost of activity targeting MantiCORE, including increased information sharing as the group became a prime focus of international law enforcement. Eventually, an international task force was set up of public sector partners supported by private sector companies to pursue offensive actions against MantiCORE. After months of hard work, the task force ultimately succeeded in seizing MantiCORE's primary websites and infrastructure, dismantling its operations, and discrediting many of the key individuals working for the gang.



*Figure 4: Fictitious MantiCORE Seizure Page*

In phase three of the scenario, facilitators encouraged participants to share ideas for the ways in which their respective organizations could contribute to an effective disruption effort.

Participants noted that the current ransomware ecosystem works particularly well to isolate victims and dissuade entities that facilitate ransom payments from collaborating openly with organizations with the power to disrupt ransomware actors.

Right now, visibility into the ransomware payment ecosystem is fragmented across many organizations, both public and private. Threat intelligence and analysis firms do not know how their information is being used, and do not know which agency has taken the lead on targeting a specific threat actor or disrupting a distinct phase of a ransomware attack. Some agencies appear to focus on fund recovery, for example, while others are working to disrupt infrastructure. Private sector actors expressed a desire to better understand who is taking what kind of actions and where they can collaborate most meaningfully based on the information they have uncovered.

Participants also discussed the issue of safe havens, specifically the concentration of cybercriminal activity in Russia. Law enforcement has a limited appetite to engage with financial institutions in Russia; they cannot take direct action in places like Moscow or other CIS countries. However, law enforcement can target over-the-counter brokers, exchanges, and behaviors to increase costs and create additional friction in the system. Once the funds are transferred out of the crypto ecosystem and back into fiat currency in a hostile jurisdiction, western law enforcement has limited ability to take action.

Participants also generally recognized that the law enforcement, threat intelligence, and incident response communities have identified proactive strategies to combat cybercrime. However, the broader cyber ecosystem remains too fragmented for key players to execute these solutions quickly and effectively enough to substantially reduce existing threats.

Finally, participants recognized the importance of continued dialogue across industry and government to build trusted relationships that can facilitate effective and timely information exchange.

## After Action Analysis

Over the course of the scenario exercise, participants quickly recognized that the incentive structures varied significantly across institutions in the ransomware information ecosystem. Prosecutors and law enforcement have traditionally sought to build a solid legal case against a criminal actor. Incident responders and intel operators, on the other hand, work to quickly mitigate and thwart the threat, stopping a victim from suffering immediate or additional harm. These differing incentives have important ramifications for information sharing and collaboration and are currently reducing the efficacy of long-term strategic disruption of ransomware activity.

## **The current ransomware ecosystem is working all too well to help perpetrators.**

The fragmented nature of the global payment ecosystem makes it easier for ransomware operators to thrive. Unfortunately, due to the ways in which ransomware actors can jurisdiction hop and target victims across different sectors, law enforcement is often put in the position of playing catch-up. Private sector entities have significant visibility into the payment space and a wealth of experience working on incident response and “follow-the-money” intelligence gathering activities, but they do not always have a good sense of where their information fits into broader law enforcement-led disruption activities. In the cyber realm, victims also tend to rely on private firms to negotiate with cybercriminals and manage the situation, bypassing law enforcement because of concerns about their reputations or fears of subsequent retaliation by threat actors.

Ransomware actors also work to further isolate the victim, taking advantage of misperceptions around law enforcement and regulation regarding privacy to cut the organization off from those who could help. Engaging victims effectively includes focusing on integrating them into communities that can help.

## **Encouraging information sharing between law enforcement and victim organizations is essential for effective ransomware response and long-term disruption.**

Victim organizations do not fully understand the role that law enforcement can play in the immediate aftermath of a ransomware attack. Many victims share a common misconception that law enforcement will disrupt a company’s operations in their efforts to mitigate an attack and might even prove more harmful than helpful. Companies also fear that investigators will uncover and misuse sensitive information.

Victims fear being “blamed” for the ransomware attack and often put off seeking help from law enforcement. Victims largely do not understand that law enforcement’s primary goal is to help disrupt the attacker, not to punish the victim organization.

Many victims also focus primarily on reputational risk: companies are concerned with clients learning about the incident and about potential regulatory repercussions, rather than initial losses from paying out a ransom. This creates negative incentives that lead many companies to pay out ransoms, ultimately increasing the profitability of the ransomware industry.

Participants emphasized that clear, detailed information about TTPs ultimately helps bolster broader ecosystem security. Incident responders benefit enormously from threat intelligence reporting that unpacks the tactics, techniques, and procedures (TTPs) of malicious actors.

Incident response firms use this information not only to help a victim recover, but also to evaluate their own internal security controls and better equip third party cyber assessment teams.

Law enforcement may not communicate with enough clarity regarding what they can offer victim organizations (e.g., information or support that could help companies recover faster). While there have been vast improvements in community engagement in recent years, many biases and prejudices still exist, and victims may not fully recognize how law enforcement can help in an unfolding crisis. Any company can fall victim to a ransomware attack; the private sector needs to know more up front about the benefits of working with law enforcement. Industry—particularly those entities with visibility into the payment ecosystem—would also benefit from knowing whether joint law enforcement operations, such as those involving law enforcement agencies or multinational efforts, are already targeting the group in question.

The Joint Cybercrime Action Taskforce (J-CAT) plays a key role in coordinating between agencies, acting as a “bridge-builder” prioritizing, initiating, and executing cross-border investigations and operations. National law enforcement agencies first share information about incidents through the Secure Information Exchange Network Application (SIENA), and the information is received and delegated to the corresponding analysis project (AP). After an internal Europol EC3 assessment, J-CAT then decides if the incident meets the threshold to initiate an investigation.

Reducing the risk posed by ransomware will ultimately require all parties involved to look beyond individual incidents and instead target the broader cybercrime ecosystem. This includes disrupting enablers like initial access brokers and malware developers that support these groups. Better information sharing between incident response teams and law enforcement can help identify supply chains, creating more opportunities for strategic disruption.

All parties can also benefit from evaluating about past successes. While the specifics may need to be kept confidential to preserve sources and methods, publicizing successful takedowns that stemmed from public-private collaboration can help to articulate the ways in which law enforcement can work closely with victim organizations, intel firms, and incident responders to dismantle threat actors. There have been a number of successful takedowns, including Operation Cronos and the dismantling of LockBit in early 2024, the Hive takedown, and actions taken against Qakbot and other botnets over the last few years. Most of these operations could not have succeeded without significant public-private cooperation. With more success stories out in the open, law enforcement and industry can help change the narrative around ransomware, nurture more trusted relationships, and help create a safer operating environment for all involved.

## Legal and regulatory barriers—both real and perceived—continue to make information sharing difficult.

In-house legal teams may be wary of broad information sharing with external parties, citing concerns about protecting attorney-client privilege and maintaining control of a rapidly-progressing situation. Attorneys may not grasp the technical realities that digital forensics and incident response (DFIR), law enforcement, and other actors face, particularly if they are not cyber specialists. Similarly, incident responders and law enforcement may not appreciate the pressures and competing priorities that in-house legal teams face. All parties can benefit from increasing their understanding of the complexities of the situation from all sides. Here, opportunities for increased collaboration and a degree of “upskilling” can be helpful, so that the practical and technical nuances of each party can be fully understood.

For example, in the UK, the Crown Prosecution Service has developed a program that creates a precedent for lawyers with cyber-specific knowledge to be points of contact and subject matter experts for the service and the rest of UK law enforcement. Another similar arrangement exists occurred in Canada where law enforcement authorities, prosecutors, and private law firms with significant experience working in cyber incident response undertook in-depth discussions of key issues and challenges associated with reporting and information sharing. These key partners then combined efforts to develop a Cyber Incident Questionnaire to assist Canadian law enforcement agencies across jurisdictions in the manner through which they undertook investigative activities that capture information from victim organizations. The document is shared proactively with Canadian private sector partners to assist them in their incident response planning, allowing them to anticipate the critical information requirements of law enforcement and enabling advance internal discussions with counsel and risk management executives on how to best engage police during a cyber incident.

Building a future case requires preserving evidence and maintaining clear lines of evidence sourcing. This does not always work well in the high-pressure, fast-moving environment following a ransomware attack. Entities may want to share information but face possible issues with GDPR or other privacy regulations. Creating additional mitigation measures to encourage cooperation with law enforcement early in exchange for leniency on other issues could encourage and strengthen earlier collaboration.

# Recommendations for Consideration

Analysis of the results from Exercise VEIL STORM reveals several potential recommendations for addressing the observed shortfalls and opportunities to enhance operational collaboration and information sharing in responding to cyber incidents.

## 1. Clarify Existing Processes

**Joint exercises can be leveraged to create more opportunities for organizations to work together.**

The security community can and should organize more cross-sector exercises between public and private actors. Smaller, scalable events, like tabletop exercises, could run simulations of ransomware attacks with key financial institutions, cloud service providers, legal professionals, incident response firms, cryptocurrency institutions, and law enforcement professions.

These kinds of activities not only help organizations develop and practice response plans but also facilitate relationship-building that becomes crucial in the event of a real incident. As emphasized by many participants at the TTX in October, the first contact between law enforcement actors and victims should not be made during a crisis. Routine engagement can better prepare all actors for future incidents should they arise.

**In an era of geopolitical uncertainty, bilateral and multilateral mechanisms for collaboration are more important than ever.**

Many states are facing shifting political realities domestically and internationally and are having to adjust resources to accommodate. Organizations need to work together to use limited resources efficiently to combat cybercrime. Entities like Europol's European Cybercrime Centre, which now has over a decade of experience collaborating on takedowns and disruptions, are now more vital than ever. Lessons learned from past incidents and disruption efforts can be shared and amplified across the community and leveraged to build more streamlined and resilient mechanisms for future incident response.



## 2. Empower People

**Work to empower the proper emissaries for creating relationships between private companies and law enforcement.**

Incident response firms can be good emissaries, particularly if they have staff with law enforcement backgrounds. Companies should be rewarded for working with law enforcement, and regulators and policymakers should take any opportunity possible to create avenues for victim organizations to reduce regulatory consequences if they opt to cooperate early and often. Attendees noted that the community has a unique opportunity to build a reputational element into the ecosystem that makes it clear that private industry gains stronger credibility when they work directly with the government in the face of a cyber incident or attack.

**Build on existing efforts, such as the NCFTA, the RTF, ISACs, and the Cybercrime Atlas.**

Public-private partnerships such as those developed through IST's RTF, FS-ISAC, and the NCFTA have already helped to create strong ties across industry and law enforcement. Particularly in the case of the finance sector, financial institutions and incident response firms are working with government regulators and law enforcement agencies on a daily basis. Creating trusted connectors between victims and law enforcement is crucial to strategically disrupt ransomware groups. Capitalizing on existing mechanisms can help jumpstart trusted relationships by expanding on what is already working, instead of creating new and potentially overlapping efforts.

## 3. Create New Mechanisms

**Explore cyber insurance as a new lever to encourage information sharing.**

Cyber insurers could play a role in requiring companies to meet certain standards following an attack. For example, an insurer could mandate a policyholder to take specific actions, such as cooperating with law enforcement. Meeting these standards would then be necessary for companies to be eligible for certain payouts. Insurers are almost always drawn into ransomware incident response and thus can be leveraged as a helpful third-party to promote better collaboration from the outset.

Some participants were skeptical about the utility of insurers taking these actions and stressed that civil society may be a more useful avenue for advocating for collaboration between authorities and victim organizations.

## **Examine the effects of sanctioning entities that facilitate money-launder operations on curtailing crime**

The proposal to sanction entities that facilitate money-laundering received mixed responses, as some organizations worried that this would put all of the liability burden on exchanges. Others also worried about focusing too closely on mixers, as they have other valid uses and can be unfairly maligned. Overall, participants agreed that the incident response and enforcement ecosystem needs to do a better job of integrating a diverse array of players into its practices and processes, which may include working with entities that have previously had a poorer record of compliance.

## **Consider introducing private sector partners into international law enforcement operations to improve communication and build relationships.**

Europol's EC3 has a strong network of private sector advisory groups that share information and best practices with law enforcement from a range of countries. However, while private industry has given presentations to the EC3 on particular threat actors, TTPs, or other lessons learned, they do not have sustained collaboration. Embedding private sector company emissaries into law enforcement agencies could help to facilitate more information sharing and also build trusted relationships. Operational sprints can be a helpful mechanism as well. Law enforcement agencies and private sector companies can come together for a short period of time to share intelligence and problem-solve in a neutral environment to advance progress on key points of friction. This type of partnership has been successful in the past in disruptions like the Trickbot and Qakbot takedowns, and should be leveraged in the future.

## **Create opportunities for private sector actors to develop close relationships with, and understanding of, law enforcement priorities and structures.**

The FBI Chief Information Security Officers (CISO) Academy can serve as one such model for other academies geared toward lawyers or other relevant professionals. The FBI initially launched the CISO academy to bring CISOs into the FBI Academy to see firsthand how agents are trained and to give these executives an opportunity to build relationships with law enforcement that can help smooth future interactions. Through this model, executives have

the opportunity to connect with law enforcement leadership, walking through scenarios and learning how law enforcement operates and responds. These kinds of academy models can help address and dispel preconceptions of how law enforcement operates in the cybercrime space.

## **Build a framework for ransomware disruption that allows for contributions from both law enforcement and private companies.**

Disrupting ransomware requires cooperation and insight from a variety of public and private sector players. Many entities, including incident response firms, threat intelligence organizations, and victims themselves may not be aware of the insights they have into the ecosystem. Developing a framework for appropriate disruption measures that can be taken by all parties—including how best to share information with law enforcement, regulators, and other authorities—would be a useful tool to catalyze more dynamic and flexible approaches to dismantling cybercriminal operations.

# Conclusion and Next Steps

This tabletop was the first in a series to be co-hosted by Europol and IST at Europol's headquarters in The Hague, the Netherlands. Owing to the success of Exercise VEIL STORM I, Exercise VEIL STORM II is set to take place on the margins of the upcoming EC3 Cybercrime Conference in the fall of 2025. This follow-on activity will take up many of the questions and challenges posed by the first exercise and further explored in this after-action report.

In particular, VEIL STORM II will focus on specific aspects of operational integration of effort between law enforcement, private sector partners, and other key stakeholders within the cybercrime ecosystem. The exercise will be centered around building out an operational plan and leveraging private sector communities more effectively. The organizing committee is also intentionally inviting a broader spectrum of private organizations and civil society organizations who can be involved with cybercrime incidents.

# Acronyms and Abbreviations

AML	Anti-money laundering
BNPL	“Buy Now, Pay Later” Services
CERT	Computer Emergency Response Team
CIS	Commonwealth of Independent States
CISO	Chief Information Security Officer
CSPs	Cloud service providers
EC3	Europol European Cybercrime Centre
EU MS	European Union Member States
DFIR	Digital Forensics and Incident Response
FBI	U.S Federal Bureau of Investigation
FS-ISAC	Financial Services Information Sharing and Analysis Center
GDPR	General Data Protection Regulation, a major EU data protection law
IOC	Indicator of compromise
IR	Incident response
IST	Institute for Security and Technology
J-CAT	Joint Cybercrime Action Taskforce
KYC	Know your customer
MSP	Managed Service Provider
NCA	UK National Crime Agency
NCA/NCCU	UK National Crime Agency - National Cyber Crime Unit
OFAC	U.S. Office of Foreign Assets Control
OFSI	UK Office of Financial Sanctions Implementation
PII	Personally Identifiable Information
RaaS	Ransomware-as-a-Service

RCMP	Royal Canadian Mounted Police
RCMP-NC3	Royal Canadian Mounted Police National Cybercrime Coordination Centre
RTF	Ransomware Task Force
SaaS	Software-as-a-Service
SAR	Suspicious Activity Report
SIENA	Secure Information Exchange Network Application (used by Europol)
TTPs	Tactics, Techniques, and Procedures
TTX	Tabletop Exercise



**INSTITUTE FOR SECURITY AND TECHNOLOGY**

[www.securityandtechnology.org](http://www.securityandtechnology.org)

[info@securityandtechnology.org](mailto:info@securityandtechnology.org)

Copyright 2025, The Institute for Security and Technology