A COMPARATIVE THREAT ASSESSMENT ON COUNTER RANSOMWARE INTERVENTIONS

A SNAPSHOT

SEPTEMBER 2024

INTERPOL

Australian Government
Department of Home Affairs

ICRTF
INTERNATIONAL COUNTER
RANSOMWARE TASK FORCE

FOREWORD

"Ransomware is a challenge that must be addressed through global partnerships, such as the Counter Ransomware Initiative (CRI). This report is a result of INTERPOL and Australia's Department of Home Affairs combined resources and expertise and provides a comprehensive review of CRI members' methodologies in countering ransomware attacks. This effort is critical to developing successful strategies that will disrupt the ransomware ecosystem and protect citizens and businesses around the world from this threat."

Jürgen Stock
INTERPOL Secretary General

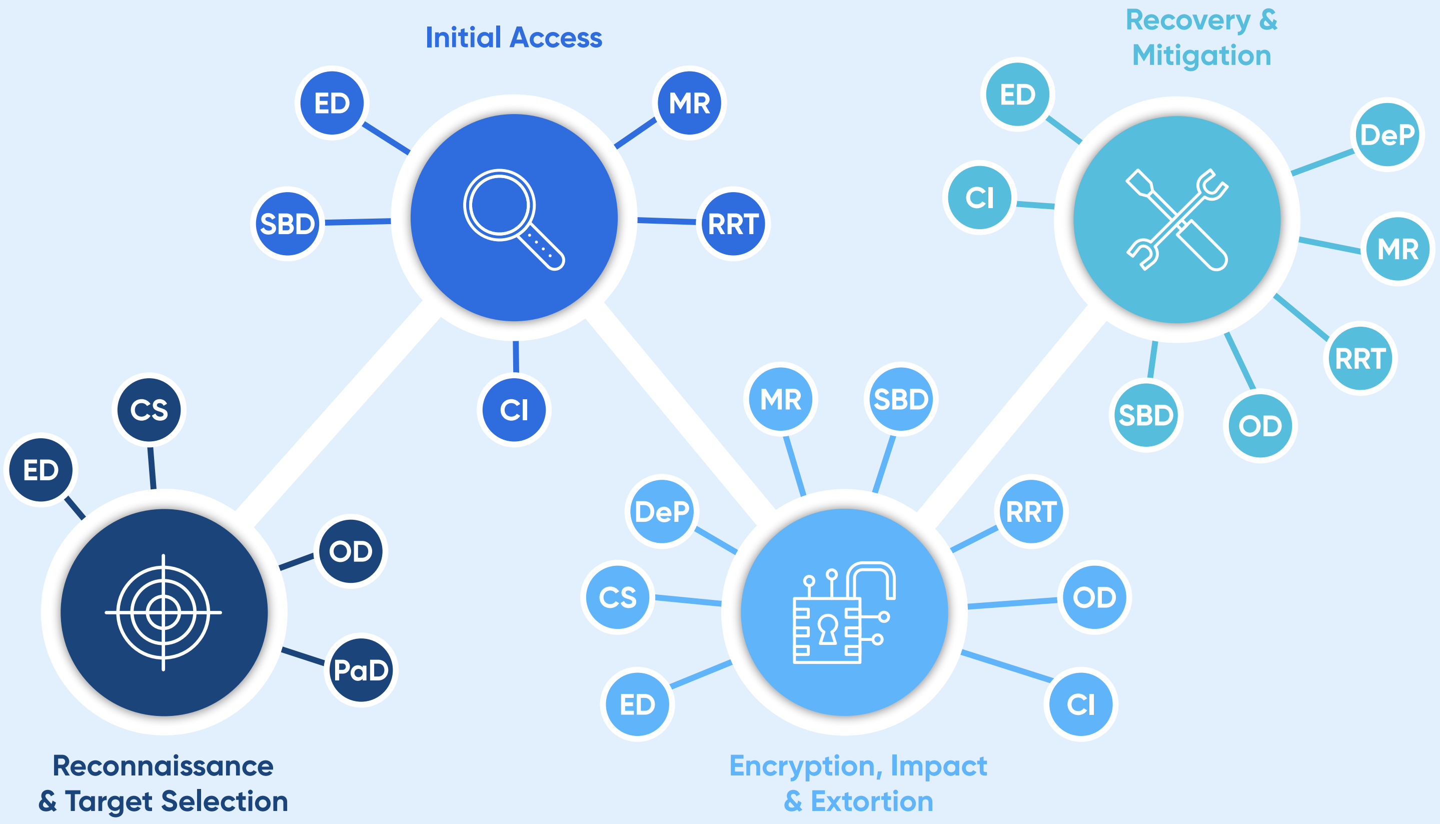
COUNTER RANSOMWARE INTERVENTIONS 2024

This Snapshot derives from "A Comparative Threat Assessment on Counter Ransomware Interventions," a study conducted within the International Counter Ransomware Initiative framework to enhance collective resilience against ransomware threats. The original assessment was completed in September 2024 and analysed various counter-ransomware interventions, identified emerging trends, and evaluated their impact on the ransomware ecosystem, while determining the optimal deployment timing within different attack stages.

Building on the collaboration between the Australian Department of Home Affairs, the Cyber Security Cooperative Research Centre, and INTERPOL, this Snapshot adapts the original findings for the broader global community, focusing exclusively on open-source information. The analysis examines multiple intervention strategies, including ecosystem disruption, cyber sanctions, decryption partnerships, mandatory reporting requirements, payment disruption, ransomware response teams, operational disruption, secure-by-design policies, and cyber insurance. Each intervention is evaluated for its strengths and limitations across the ransomware attack lifecycle, from reconnaissance and initial access through to encryption and extortion.

The Snapshot concludes with key requirements and recommendations for building a robust ransomware response framework.

MAPPING CURRENT INTERVENTIONS AGAINST THE PHASES OF RANSOMWARE



INTERVENTIONS

ED	Ecosystem disruption
CS	Cyber sanctions
DeP	Decryption partnerships
MR	Mandatory reporting
PaD	Payment disruption
RRT	Ransomware response teams
OD	Operational disruption
SBD	Secure-by-Design policies
CI	Cyber insurance

🔵 INTERVENTION PROS ⚫ INTERVENTION CONS

	RECONNAISSANCE AND TARGET SELECTION	INITIAL ACCESS	ENCRYPTION, IMPACT AND EXTORTION	RECOVERY AND MITIGATION
ECOSYSTEM DISRUPTION Changes to the cybercriminal ecosystem by threat actor action	Can lead to changes in targeting patterns: what and who to target are key causes of mistrust between different affiliates and threat actors.	Can result in some service providers being less trusted or unable to provide their services. Criminals may not have access to breached credential databases.	Ransomware operations rely heavily on infrastructure during this phase: if an event occurs in the ecosystem which creates mistrust towards a specific group, their operations are less likely to be trusted.	Exit scams between groups can disrupt the publishing of breached data.
	This is unlikely to stop or disrupt ransomware targeting, but simply shift it.	Criminals will quickly identify new sources for services.	Ecosystem disruption cannot be predicted and is unlikely to have a tangible impact on a recent attack.	Cannot be predicted or counted upon; disruption may lead to a double ransomware claim.
CYBER SANCTIONS Government-controlled orders against threat actors or associated services	May discourage criminal groups from targeting specific areas or countries to avoid sanctions.	N/A	May be able to disrupt the payment ecosystem by sanctioning cryptocurrency payment operations.	N/A
	May encourage groups to target specific areas or countries to express defiance of sanctions.		Sanctions cannot prevent attacks at the point of encryption.	
DECRYPTION PARTNERSHIPS Cross-organisation partnerships to provide free decryption tools	N/A	N/A	Can assist in providing organisations with universal encryption keys and allowing companies to decrypt data.	Sharing decryption keys can assist in recovery of data.
			Cannot prevent initial encryption and the exfiltration and publishing of exfiltrated data.	The availability of some decryption keys is limited.
MANDATORY REPORTING REQUIREMENTS Legislation requiring organisations to report a ransomware attack	N/A	Could identify when a breach or credential leak has occurred, forcing an organisation to change its security posture.	Will be able to build a clearer picture of targeting by group and by sector.	Will assist in providing a more detailed database of attacks and can encourage industry peer support.
		Are dependent on the country where attacks occur; still much discussion on what circumstances constitute mandatory reporting.	Cannot prevent initial encryption and the exfiltration and publishing of exfiltrated data.	Will increase the complexity of ransomware response, which without clear delineations of responsibility may make the initial incident response slower.
PAYMENT DISRUPTION Measures to prevent ransom payment	May discourage groups from targeting certain countries.	N/A	May prevent groups from encrypting data and issuing ransom demand if there is a no payment policy.	N/A
	May encourage groups to target certain companies to use as part of an extortion strategy.		May encourage groups to exfiltrate sensitive data and sell it or use it in further intrusions.	
RANSOMWARE RESPONSE TEAMS Public-private partnerships to deploy in a ransomware attack	N/A	May be able to assist an organisation at the initial part of the breach.	Can assist in negotiations and mitigation once an attack has happened.	Can provide key assistance in recovery and mitigation during a ransomware attack using experts across the private and public sector.
		The initial access would have to be immediately identified by the organisation's SOC or security partner.	Teams may be limited by timing and ability to deploy once an initial intrusion has been detected.	Currently reliant on a limited number of experts, and unlikely to meet current ransomware demands.
OPERATIONAL DISRUPTION Law Enforcement action against a threat actor	Previous disruption operations may limit the targeting of a specific sector or a specific geographic area.	N/A	May be able to prevent exfiltrated data from being published by seizing servers and assisting in decryption.	May be able to provide organisations with decryption keys and wipe data in this phase. Given an increase in some organisations not knowing what ransomware variant has targeted them, this may increase visibility and chance of a successful recovery.
	This is unlikely to prevent targeting at the early stage of an attack		Are unlikely to assist in the active phases of a ransomware attack, or at point of encryption.	Limited to Law Enforcement action, which may take a significant period of time to conduct.
SECURE-BY-DESIGN STRATEGY The implementation of security best practices at the point of design	N/A	Should decrease the number of credential breaches and system vulnerabilities available.	Can assist in preventing the lateral movement within systems needed to deploy the ransomware.	Implementation can increase the ability to isolate the impacted segments and decrease operational downtime.
		Remains optional: organisations must make a proactive effort to teach cyber hygiene.	Must already be implemented, and may be limited once data is encrypted/exfiltrated.	Remains optional.
CYBER INSURANCE Insurance policies intended to reward good cyber practices	N/A	May be able to influence organisations to implement better security or Secure-by-Design principles.	Can assist in influencing good practices at the time of ransom demand, and can provide best practice on payment of ransomware and data breach notifications.	Can assist in influencing good practices across recovery.
		Likely to remain optional	Remains optional; unlikely to assist at point of encryption and exfiltration.	Limited in ability to assist companies technically.

CONCLUSIONS

LIMITATIONS AND LONG-TERM CHALLENGES:

No single solution has been effective against ransomware. As attackers evolve and use more sophisticated methods, defence strategies must also adapt and innovate. There is a need for long-term plans to tackle the root causes of ransomware.

THE NEED FOR DIVERSE INTERVENTIONS:

Various strategies are currently in use, including ecosystem disruption, cyber sanctions, decryption partnerships, mandatory reporting, payment disruption, RRTs, and secure-by-design policies.

This variety shows:

The complexity and breadth of the ransomware threat;

The need for a multi-layered approach;

The potential risk for duplication of efforts and the need to target relevant efforts at all stages of a ransomware attack.

THE NEED FOR COMPREHENSIVE STRATEGIES AND COLLECTIVE ACTION:

A global strategy that combines legal, technical, and policy measures is crucial. Furthermore, international cooperation and information sharing are essential to disrupt the ransomware ecosystem effectively.

Given the above and in line with the original report,[1] this Snapshot recommends that member countries strengthen the sharing of lessons learned through interventions applied, their strengths and limitations, to facilitate the creation of a comprehensive global strategies seeking to disrupt ransomware operations.

[1] The original report titled "A Comparative Threat Assessment on Counter Ransomware Interventions" is available on the internal website of the International Counter-Ransomware Initiatives for all members.