# Incident Response Action Card Ransomware

**Version:1**

**22 December 2022**

## 1 Scope

1.1 This document applies whenever the security of an ICT system or data is impacted, or has the potential to be impacted, by a ransomware threat.

1.2 The action card is intended for use by operational officers, primarily within ICT and [response] teams. All ICT individuals who participate within incident response can adopt and use this action card where appropriate.

1.3 The guidance in this action card expands on and must be read in conjunction with the internal Council Cyber Security Incident Processes and Procedures. Adherence to guidance within both documents is required for effective Incident Response.

1.4 Any contractual, legal or government regulatory requirements mandating more stringent requirements than specified in this action card will supersede the requirements of this document.

## 2 Ransomware Definition

2.1 Ransomware is a type of malicious software in which the data on a victim's computer is locked, typically by encryption, and payment is demanded before the ransomed data is decrypted and access is returned to the victim. The motive for ransomware attacks is nearly always monetary, and unlike other types of attacks, the victim is usually notified that an exploit has occurred and is given instructions on how to recover from the attack

## 3 Baseline Recommendations

3.1 **Retain a full audit trail** of your actions to avoid problems in a criminal case.

3.2 **Implement the Triage phase** immediately wherever possible.

3.3 **Implement the Triage and Contain phases** swiftly to avoid further criminal damage including system breaches and data loss.

3.4 **Process assets individually through phases** to avoid undue delays which increase the incident severity – i.e., do not wait for full information before acting.

3.5 **Implement the Analysis and Search phases comprehensively** to avoid persistent criminal presence within Council systems.

3.6 **Defer the Recovery phase until the Isolate phase is** complete to avoid persistent criminal presence within Council systems.

3.7 **Regularly update on situation** to avoid undue delays which cause the Council to breach legal requirements.

## Incident Discovery:

**What should you do if a suspected ransomware threat is reported/uncovered?**

**Immediate**

*Triage*

- **Aim-** *Record the incident details and obstruct obvious threats.* Monitor detection channels, both automatic and manual, customer and staff channels for the identification of a malware attack, including:
- Anti-malware system notifications to the IT team (unable to update its signatures, shutting down or unable to run manual scans.)
- User notification to the Service Desk;
- Any other notification that raises suspicion of a ransomware incident.

The creation for the above, could include, but is not limit too:

- Anti-spam or email filters alerts
- Anti-virus software alerts
- Anti-spam browser plug-in alerts
- EDR solution alerts – most advance threats are polymorphic to bypass anti-virus or other protection layers deployed in an enterprise's environment. By focusing on generic signature detection mechanism may not good enough to detect the attacks.
- SIEM alerts and correlated event alerts
- File integrity checking software alerts
- Operating system, service and application logs
- High volume of exceptional network or hard disk activities
- Abnormal network flows and alerts
- Alerts of Command and Control (C2) traffic from a compromised host
- Informed by end users when they saw the ransom note or encrypted files
- Informed by SOC analysts or law enforcement 1.2 Detection and Identification

Ransomware will usually not try to hide.

- Popped-up ransom note onscreen
- Personal files (images, movie, files, documents, text files) were encrypted with unique extension
- Network drive folders or files on USB connected NAS devices encrypted
- Infected system was locked due to some system libraries was encrypted
- Infected system crashed due to some system libraries was encrypted
- Services disrupted due to some application libraries was encrypted

- Annoying message of pornographic images displayed and not able to remove
- For a Windows system that is joined to an Active Directory (AD) domain, files in a user's 'roaming profiles may also be encrypted. Responder needs to investigate if there are any other files (images, movie, files, documents, text files) of the investigating system were encrypted. If some files are not encrypted, there is a possibility that ransomware was not executed on this system