West Lindsey DISTRICT COUNCIL

Incident Response Action Card Malware

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 malware 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 Malware Definition

2.1 Malware is any software intentionally designed to negatively impact a computer, server, client, or computer network. Malware must be implanted or introduced in some way into a target's computer. Malware can take the form of executable code, scripts, active content, and/or other software.

Malware can include computer viruses, worms, trojan horses, spyware, rootkits, botnet software, keystroke loggers, ransomware, crypto miners, adware and malicious mobile code. Some types of malware (e.g., spyware, rootkits, ransomware, crypto miners and botnet software) are often used during sophisticated cyber-attacks against organisations. In these cases, malware can be customised to target specific systems within an organisation’s technical infrastructure and configured to avoid detection. Malware has a malicious intent, acting against the interest of the computer user and so does not include software that causes unintentional harm due to some deficiency, which is typically described as a software bug.

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.

4 Detect or reported incident:

- **Implement the Analysis and Search phases comprehensively** to avoid persistent criminal presence within Council systems.
- **Defer the Recovery phase until the Isolate phase is complete** to avoid persistent criminal presence within Council systems.
- **Regularly update on situation** to avoid undue delays which cause the Council to breach legal requirements.

5 What should you do if a suspected phishing 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 malware incident.

- o Unusual hard-disk activity: the hard drive makes huge operations at unexpected times
- o Unusually slow computer: sudden unexplained slowdowns not related to system usage.
- o Unusual network activity: slow internet connection/ poor network share performance at irregular intervals.
- o Computer rebooting without reason.
- o Applications crashing unexpectedly.
- o Pop-up windows appearing while browsing the web (possible without browsing)
- o Full description, impact and scope.

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

- Physical and logical locations including [asset].
- LAN and internet applications with a user login.
- Record outcomes of actions above.

Identify likelihood of widespread malware infection.

- Physical and logical locations including [asset].
- Assign an Incident Severity
- Assign an Incident Category

Malware samples are unsafe and should be handled with extreme care.

6 If at this point if a potential compromise is suspected:

Obstruct any clearly identified threats and preserve evidence for analysis:

- Disconnect endpoint network cable & wireless.
- Disconnect the power cable.