RakshaSutraX Incident Response

Malware Playbook v1.0

Document Control

Title	Malware Playbook
Version	1.0
Date Issued	0112/2024
Status	Draft
Document owner	RaptorX7
Creator name	RaptorX7
Creator organisation name	RakshaShutraX
Subject category	Cyber Incident Response Management
Access constraints	

Document Revision History

Version	Date	Author	Summary of changes
1.o	01/012/2024	RaptorX7	Generic Version Created from Public Sector Playbook

Contents

1. Introduction

1.1. Overview

In the event of a cyber incident, it is important that the organisation is able to respond, mobilise and execute an appropriate level of response to limit the impact on the brand, value, service delivery and the public, client and customer confidence. Although all cyber incidents are different in their nature and technologies used, it is possible to group common cyber incident types and methodologies together. This is in order to provide an appropriate and timely response depending on the cyber incident type. Incident specific playbooks provide incident managers and stakeholders with a consistent approach to follow when remediating a cyber incident.

References are made to both a Core IT CIRT and a CIRT within this document. This is in recognition the playbook will be used by organisations of different sizes. Some may initially manage an incident with a small response team within IT services but where there is a confirmed compromise this may be escalated to an extended level CIRT comprising of members of the organisation outside the IT services who will deal with agreed categories of compromise. The Playbook as with the Cyber Incident Response Plan CIRP will require to be adjusted to reflect the organisational make up.

Playbooks describe the activities of those directly involved in managing specific cyber incidents. However, it is important to acknowledge the speed at which cyber incidents can escalate and become a significant business disruptor requiring both business continuity and consequence management considerations. Early consideration should be given to engaging Business Continuity, Resilience and Policy Area Leads in order that the wider issues can be effectively managed. Business Continuity and Resilience leads within the organisation must therefore be familiar with the CIRP and Playbooks and how they link to wider Incident response and Exercising Playbooks and arrangements.

1.2. Purpose

The purpose of this Cyber Incident Response: Malware Playbook is to define activities that should be considered when detecting, analysing and remediating a malware incident. The playbook also identifies the key stakeholders that may be required to undertake these specific activities.

1.3. Malware Definition

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, cryptominers, adware and malicious mobile code. Some types of malware (e.g. spyware, rootkits, ransomware, cryptominers 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 thus does not include software that causes unintentional harm due to some deficiency, which is typically described as a software bug.

1.4. Scope

This document has been designed for the sole use of the first responders such as the Service Desk team when responding to a cyber incident. It is not standalone and must be used alongside the CIRP.

1.5. Review Cycle

This document is to be reviewed for continued relevancy by the Cyber Incident Response Team (CIRT) lead at least once every 12 months; following any major cyber security incidents, a change of vendor, or the acquisition of new security services.

2. Preparation Phase

Preparation Phase		
Phase objectives	The preparation phase has the following objectives: • Prepare to respond to cyber security incident in a timely and effective manner; • Prepare organisational assets for malware outbreak; • Inform employees of their role in remediating a malware incident including reporting mechanisms.	
Activity	**Description**	**Stakeholders**
Prepare to respond	Activities may include, but are not limited to:	
	Ensure that: • All desktop/laptop and server systems have an anti-malware solution deployed. • Gateway anti-malware solutions are in place. • Users are encouraged to store data on shared drives that are backed up and not on local device drives. • Local admin rights have been removed as far as currently practical.	• Information Security Manager • Head of IT
	Review and rehearse cyber incident response procedures including technical and business roles and responsibilities, escalation to major incident management where necessary.	• Head of Information Governance • Head of IT • Information Security Manager • Team Leader • Service Delivery Manager • Service Desk Analysts/Technicians • Legal Team

		• Communications Team • Resilience Lead • Business Continuity Lead
	Review recent cyber security incidents and the outputs.	• Information Security Manager
	Review threat intelligence for threats to the organisation, brands and the sector, as well as common patterns and newly developing risks and vulnerabilities.	• Information Security Manager
	Ensure appropriate access to any necessary documentation and information, including out-of-hours access, for the following: • CIRP; • Network Architecture Diagrams • Data Flow Diagrams	• Information Security Manager
	Identify and obtain the services of a 3rd party Cyber Forensic provider.	• Information Security Manager
	Define Threat and Risk Indicators and Alerting pattern within the organisation's security information and event management (SIEM) solution.	• Information Security Manager
Activity	**Description**	**Stakeholders**
Inform employees	Activities may include, but are not limited to:	
	Conduct regular awareness campaigns to highlight information security risks faced by employees, including: • Phishing attacks and malicious emails; • Ransomware;	• Head of IT • Information Security Manager • Resilience Lead • Business Continuity Lead

	• Reporting a suspected cyber incident.	
	Ensure regular security training is mandated for those employees managing personal, confidential or high risk data and systems.	• Head of IT • Information Security Manager • HR • L&D Department • Resilience Lead • Business Continuity Lead

3. Detect

Detection Phase		
Phase objectives	The detection phase has the following objectives: • Detect and report a breach or compromise of the confidentiality, integrity or availability of organisational data; • Complete initial investigation of the malware; • Report the malware formally to the correct team as a cyber incident.	
Activity	**Description**	**Stakeholders**
Detect and report the incident	Activities may include, but are not limited to:	
	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; • User notification to the Service Desk; • Any other notification that raises suspicion of a malware incident. **Isolated malware infections are to be expected from time to time and will normally be dealt with automatically by the anti-malware technology implemented by the organisation. It is only if an outbreak is impacting on services that the cyber incident response process and this playbook will be engaged.*	• Information Security Manager • Core IT CIRT
	Report the cyber incident via the Service Desk. If a ticket does not exist already, raise a ticket containing minimum information. To report an incident, follow the process defined in the CIRP.	• Information Security Manager • Core IT CIRT

	Consider reporting to Police Scotland where criminal Investigation may be warranted	
	Consider whether data loss or data breach has occurred and if so refer to data breach playbook.	• Information Security Manager • Information Governance Team • Core IT CIRT
	Classify the cyber security incident, based upon available information related to the malware attack the incident types **(see CIRP).**	• Information Security Manager • Core IT CIRT
	Report the cyber incident in accordance with the organisation's CIRP. Consider the Intelligence value to other organisations and share on the CiSP	• Information Security Manager • Core IT CIRT • CIRT
	Where appropriate consider reporting requirements to Information Commissioner's Office (ICO), relevant Regulator and or Competent Authority (NISD), National Cyber Security Centre (NCSC) and / or Police Scotland	• Information Security Manager • Core IT CIRT • CIRT
Activity	**Description**	**Stakeholders**
Initial investigation of the incident	Activities may include, but are not limited to:	
	Mobilise the CIRT to begin initial investigation of the cyber security incident **(see staff contact details within CIRP).**	• Information Security Manager • CIRT

		The following may also be included in the incident response team where appropriate for the incident: • Service Desk Analysts • Server Desk Technicians • Server Team • Mobile Device Team
	Identify likelihood of widespread malware infection.	• Head of IT • Information Security Manager • Core IT CIRT • CIRT
	Collate initial incident data including as a minimum for following; • A timeline of when the malware was first detected, and other significant events. • Whether the malware was detected by the anti-malware solution, or identified through other means. • The probable scope of the infection, in terms of the systems and/or applications affected. • Whether the malware appears to be spreading across the infrastructure. • The probable nature of the malware infection, if known. • Whether the anti-malware solution has successfully quarantined/cleansed the infection. • Likely containment options (e.g. on the basis of publicly-available information, for known malware).	• Head of IT • Information Security Manager • Core IT CIRT • CIRT
	Secure artefacts, including copies of suspected malicious software and forensic copies of affected system(s) for future analysis.	• Information Security Manager • Core IT CIRT

	Research Threat Intelligence sources and consider Cyber Security Information Sharing Partnership (CiSP) submission to gain further intelligence and support mitigation by others.	• Information Security Manager • Core IT CIRT
	Review cyber incident categorisation to validate the cyber security incident type as a malware attack and assess the incident priority, based upon the initial investigation. (**See CIRP for Incident Severity Matrix)**	• Security Manager • Core IT CIRT
Activity	**Description**	**Stakeholders**
Incident reporting	Activities may include, but are not limited to:	
	Report the cyber incident in accordance with the organisation's CIRP.	• Information Security Manager • CIRT
	Report the Cyber incident in accordance with the organisation's CIRP. Consider the Intelligence value to other organisations and share on the Cisp	• Information Security Manager • Core IT CIRT • CIRT
	Where appropriate consider reporting requirements to Information Commissioner's Office (ICO), relevant regulator and or Competent Authority (NISD), National Cyber Security Centre (NCSC) and / or Police Scotland	• Information Security Manager • Core IT CIRT • CIRT
	Escalate in accordance with the CIRP.	• Information Security Manager • CIRT • Resilience Lead • Business Continuity Lead

Activity	Description	Stakeholders
Establish the requirement for a full forensic investigation	Activities may include, but are not limited to:	
	Consider conducting a full forensic investigation, on the advice of legal counsel. All evidence handling should be done in line with the Association of Chief Police Officers (ACPO) Good Practice Guide for Digital Evidence.	• Information Security Manager • Core IT CIRT • CIRT

4. Analyse

Analysis Phase		
Phase objectives	The analysis phase has the following key objectives: • Analyse the cyber incident to uncover the scope of the attack; • Identify and report potentially compromised data and the impact of such a compromise; • Establish the requirement for a full forensic investigation; • Develop a remediation plan based upon the scope and details of the cyber incident.	
Activity	**Description**	**Stakeholders**
Analyse the extent of the incident	Activities may include, but are not limited to:	
	Engage technical staff from resolver groups.	• Service Desk Technicians • Core IT CIRT

	Classify the malware by submission to multiple AV vendors and determine the family it belongs to.	• Information Security Manager • Core IT CIRT
	Scope the attack. • A timeline of when the malware was first detected, and other significant events. • Whether the malware was detected by the anti-malware solution, or identified through other means. • The probable scope of the infection, in terms of the systems and/or applications affected. • Whether the malware appears to be spreading across the infrastructure. • The probable nature of the malware infection, if known. • Whether the anti-malware solution has successfully quarantined/cleansed the infection. • Likely containment options (e.g. on the basis of publicly-available information, for known malware).	• Information Security Manager • Core IT CIRT • CIRT
	Reverse-engineer the malware in a secure environment to understand its mechanisms, and the functionality it implements.	• Information Security Manager • Core IT CIRT • CIRT
	Execute the malware in a secure environment or sandbox, segregated from the business network, to determine its behaviour on a test system, including created files, launched services, modified registry keys and network communications.	• Information Security Manager • Core IT CIRT
	Review affected infrastructure for indicators of compromise derived from the malware analysis to identify any additional compromised system(s).	• Information Security Manager • Core IT CIRT
	Preserve all evidence to support attribution or anticipated legal action.	• Information Security Manager • Core IT CIRT

		• CIRT
	Examine threat intelligence feeds to determine if the malware attack is bespoke and targeted at specific accounts, infrastructure or systems.	• Information Security Manager • Core IT CIRT
	Verify all infected assets are in the process of being recalled and quarantined.	• Information Security Manager • Core IT CIRT • CIRT

5. Remediation – Contain, Eradicate and Recover

Remediation Phase		
Phase objectives	The remediation phase has the following objectives: • Contain the effects of the malware on the targeted systems; • Eradicate the malware from the network through agreed mitigation measures; • Recover affected systems and services back to a Business As Usual (BUA) state.	
Activity	**Description**	**Stakeholders**
Containment	Contain the technical mechanisms of the malware attack, including:	
	Monitor for any new infections which might suggest that the malware is spreading across the infrastructure, and alert the CIRT to any significant changes in the scope of the incident (e.g. the infection of a previously unaffected business system or site).	• Information Security Manager • Core IT CIRT
	Ensure that the latest malware definitions have been deployed across the anti-malware solution.	• Information Security Manager • Core IT CIRT
	Initiate an estate-wide anti-malware scan.	• Information Security Manager • Core IT CIRT
	Identify the infected assets(s) and physically disconnect them from the network. Business continuity options for users affected by such disconnection include:	• Information Security Manager • Core IT CIRT

	• Replacing disconnected devices with fresh builds from IT, where stocks permit (ensuring they first have relevant updates applied). • Directing users whose devices are disconnected to work from an alternative location; such as another office, a Disaster Recovery facility or from home. Where necessary the corporate disaster recovery process will be followed.	
	Determine whether the malware appears to be attempting to communicate with outside parties (e.g. attempting to connect to botnet command and control servers on the public internet), and take steps to block any such communication.	• Information Security Manager • Core IT CIRT • CIRT
	Suspend the login credentials of suspected compromised accounts.	• Information Security Manager • Core IT CIRT • CIRT
	Secure copies of the malicious code, affected systems and any identified artefacts for further investigation (engaging with forensic support if forensic copies are required).	• Information Security Manager • Core IT CIRT
	Inform business data owner(s) and stakeholders of the progress of containment activities.	• Information Security Manager • CIRT • Resilience Lead • Business Continuity Lead • Policy Area Lead
Activity	**Description**	**Stakeholders**

Eradication	Activities may include, but are not limited to:	
	Identify removal methods from the results of the malicious code analysis and trusted sources (AV providers).	• Information Security Manager • Core IT CIRT
	Complete an automated or manual removal process to eradicate malware or compromised executables using appropriate tools.	• Information Security Manager • Core IT CIRT
	Conduct a restoration of affected networked systems from a trusted back up.	• Information Security Manager • Core IT CIRT
	Re-install any standalone systems from a clean OS back-up before updating with trusted data back-ups.	• Information Security Manager • Core IT CIRT
	Change any compromised account details.	• Information Security Manager • Core IT CIRT
	Continue to monitor for signatures and other indicators of compromise to prevent the malware attack from re-emerging.	• Information Security Manager • Core IT CIRT
	Confirm policy compliance across the estate.	• Information Security Manager • Core IT CIRT
Activity	**Description**	**Stakeholders**
	Activities may include, but are not limited to:	

Recover to BAU	Recover systems based on business impact analysis and business criticality.	• Information Security Manager • Core IT CIRT
	Complete malware scanning of all systems, across the estate.	• Information Security Manager • Core IT CIRT
	Re-image systems.	• Information Security Manager • Core IT CIRT
	Re-set the credentials of all involved system(s) and users account details.	• Information Security Manager • Core IT CIRT
	Reintegrate previously compromised systems.	• Information Security Manager • Core IT CIRT
	Restore any corrupted or destroyed data.	• Information Security Manager • Core IT CIRT
	Restore any suspended services.	• Information Security Manager • Core IT CIRT
	Establish monitoring to detect further suspicious activity.	• Information Security Manager • Core IT CIRT
	Co-ordinate the implementation of any necessary patches or vulnerability remediation activities.	• Information Security Manager • Core IT CIRT

6. Post Incident

Post-Incident Activities Phase		
Phase objectives	The post-incident activities phase has the following objectives: • Complete an incident report including all incident details and activities; • Complete the lessons identified and problem management process; • Publish appropriate internal and external communications.	
Activity	**Description**	**Stakeholders**
Incident reporting	Draft a post-incident report that includes the following details as a minimum: • Details of the cyber incident identified and remediated across the network to include timings, type and location of incident as well as the effect on users; • Activities that were undertaken by relevant resolver groups, service providers and business stakeholders that enabled normal business operations to be resumed; • Recommendations where any aspects of people, process or technology could be improved across the organisation to help prevent a similar cyber incident from reoccurring, as part of a formalised lessons identified process.	• Senior Stakeholders • Head of Information Governance • Head of IT • Audit Committee • Information Security Manager
Lessons Identified & Problem Management	Complete the formal lessons identified process to feedback into future preparation activities.	• Information Security Manager • CIRT • Resilience Lead

	Consider sharing lessons identified with the wider stakeholders where relevant	• Information Security Manager • CIRT • Resilience Lead • Business Continuity Lead
	Conduct root cause analysis to identify and remediate underlying vulnerabilities.	• Information Security Manager • CIRT
Human Resources	Review staff welfare; working hours, over time, time off in lieu (TOIL) and expenses.	• Information Security Manager • HR
Communications	Activities may include, but are not limited to:	
	Publish internal communications in line with the communications strategy to inform and educate employees on malware attacks and security awareness.	• Information Security Manager • CIRT • Communications • Resilience Lead • Business Continuity Lead
	Publish external communications, if appropriate, in line with the communications strategy to provide advice to customers, engage with the market, and inform press of the cyber incident. These communications should provide key information of the cyber incident without leaving the organisation vulnerable or inciting further malware attacks.	• Head of IT • Information Security Manager • Communications Team

7.Annex A: Flow Diagram