Malware Incident response plan 01:

2022-04-26

This Incident Response Plan (IRP) has been prepared to support the Digital Transformation Agency (DTA) CloudSystem. The document provides guidance for responding to cyber security incidents that may occur in relation to an Agency's operation of the CloudSystem.

Purpose

The purpose of this IRP is to provide guidance to Agencies operating the CloudSystem including how to detect cyber security incidents, how to respond and remediate them, along with how to reduce the risk of an incident re-occurring in the future.

Scope

The scope of this IRP is specific to the use of Microsoft 365 services as part of the CloudSystem. As such it is termed a system-specific IRP and is designed to be subordinate to an Agency's overarching IRP. As a result, this IRP does not directly address topics that it is reasonable to assume are discussed in an Agency-level IRP.

The CloudSystem IRP is a living document. It is anticipated that, over time, amendments and updates will be applied to the CloudSystem IRP specific to agency business needs and lessons learnt from cyber incidents.

Incident response plan

This IRP is based on the four step National Institute of Standards and Technology (NIST) incident response life cycle as documented in Special Publication 800-61 Revision 2. The four steps of the process are illustrated in Figure 1 and are:

- Preparation
- Detection & Analysis
- Containment, Eradication, and Recovery
- Post-Incident Activity.

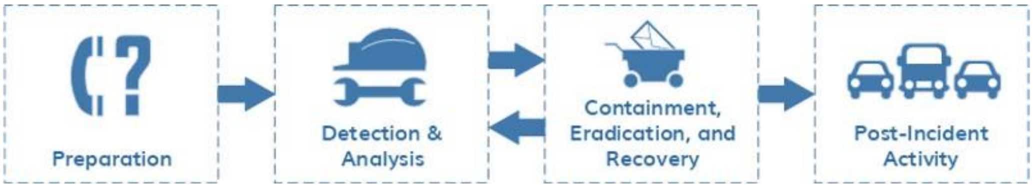


Figure 1 Incident Response Process

Each of the four incident response phases are detailed in the following sections of this document.

Preparation

The preparation phase of the incident response life cycle is a shared responsibility between the project team and Agency cyber security personnel. The project team is responsible for the design, implementation, and security assessment of the solution. This includes performing a risk assessment and determining which specific Information Security Manual (ISM) controls to implement to reduce and manage the risk of security incidents. The following documentation has been produced for the CloudSystem and it is recommended that the Agencies cyber security personnel familiarise themselves with the content to aid them in their preparation to manage an incident:

- DTA – Blueprint – Solution Overview which describes the solution, which features have been enabled/disabled for the Agency, and how the solution has been structured.
- DTA – Blueprint – Platform Design which describes the technologies used that make up the 'platform' portion of the solution and how they are implemented.
- DTA – Blueprint – Client Devices Design which describes the technologies used that make up the Windows 10 portion of the solution and how it is implemented.
- DTA – Blueprint – Office 365 Design which describes the technologies used that make up the Office 365 portion of the solution and how it is implemented.
- DTA – Cloud-Only Blueprint – Security Risk Management Plan (SRMP) which includes the details of the risk assessment performed and the recommended treatments.
- DTA – Cloud-Only Blueprint – System Security Plan (SSP) which describes how controls identified in the SSP Annex are implemented by the system.
- DTA – Cloud-Only Blueprint – System Security Plan Annex (September 2021) which states the compliance of the solution with the September 2021 version of the ISM.
- DTA – Cloud-Only Blueprint – Security Standard Operating Procedures which describe the steps required to perform multiple operational tasks within the environment.

In addition to having ongoing access to the above documentation it is assumed that Agency cyber security personnel have access to tools and resources as described in the Agency IRP.

Specific resources that are also required by Agency cyber security personnel to detect and respond to security incidents include:

- Access to the various Microsoft management portal required to administer the CloudSystem, as listed below in Table 1
- Membership of the role(s) required to perform any actions related to the incident

Table 1 Microsoft Management Portals

Portal	URL
Microsoft 365 Defender portal	https://security.microsoft.com
Defender for Cloud Apps portal	https://portal.cloudappsecurity.com
Azure portal (including Azure AD)	https://portal.azure.com
Microsoft 365 compliance portal	https://compliance.microsoft.com
Microsoft 365 admin center	https://admin.microsoft.com/

Detection and analysis

Multiple detection methods are available to the Agency's cyber security personnel to aid them in discovering and categorising security incidents. These detection methods include:

- Alerts from Azure AD (including Azure AD Identity Protection) including risky sign-ins and users flagged for risk.
- Azure AD logs stored in Azure and available via the portal, including the audit log for all administrative activities relating to Azure AD.
- Defender for Office 365 alerts and reports for each of the configured capabilities including Safe Attachments, Safe Links, Safe Attachments for SharePoint, OneDrive and Microsoft Teams, and Anti-phishing in Defender for Office 365 protection.
- Microsoft Defender for Endpoint including the Security Operations, Incidents, and Alerts Queue dashboards which provide tailored information and actions for cyber security personnel.
- Microsoft Defender for Cloud Apps Threat Detection, Privileged Accounts, and Access Control dashboards spanning the whole Microsoft 365 deployment, along with configurable email alerts and automatic response capabilities.
- Local Windows 10 events logs written to each Windows 10 endpoint including authentication attempts, firewall activities, and Windows Defender Application Control (WDAC) events.

Due to its containment, eradication and recovery capabilities in addition to its detection and analysis functionality, Microsoft Defender for Endpoint is the primarily incident response tool for the CloudSystem and is described in further detail in the section below.

Microsoft Defender for Endpoint

The CloudSystem leverages Microsoft Defender for Endpoint to monitor, detect, investigate, and respond to threats targeting Windows 10 endpoints. When an alert is triggered of sufficient severity, an email is automatically sent to a specified recipient email address (typically the Agency cyber security team mailbox or similar). Additional email recipients can be configured as required.

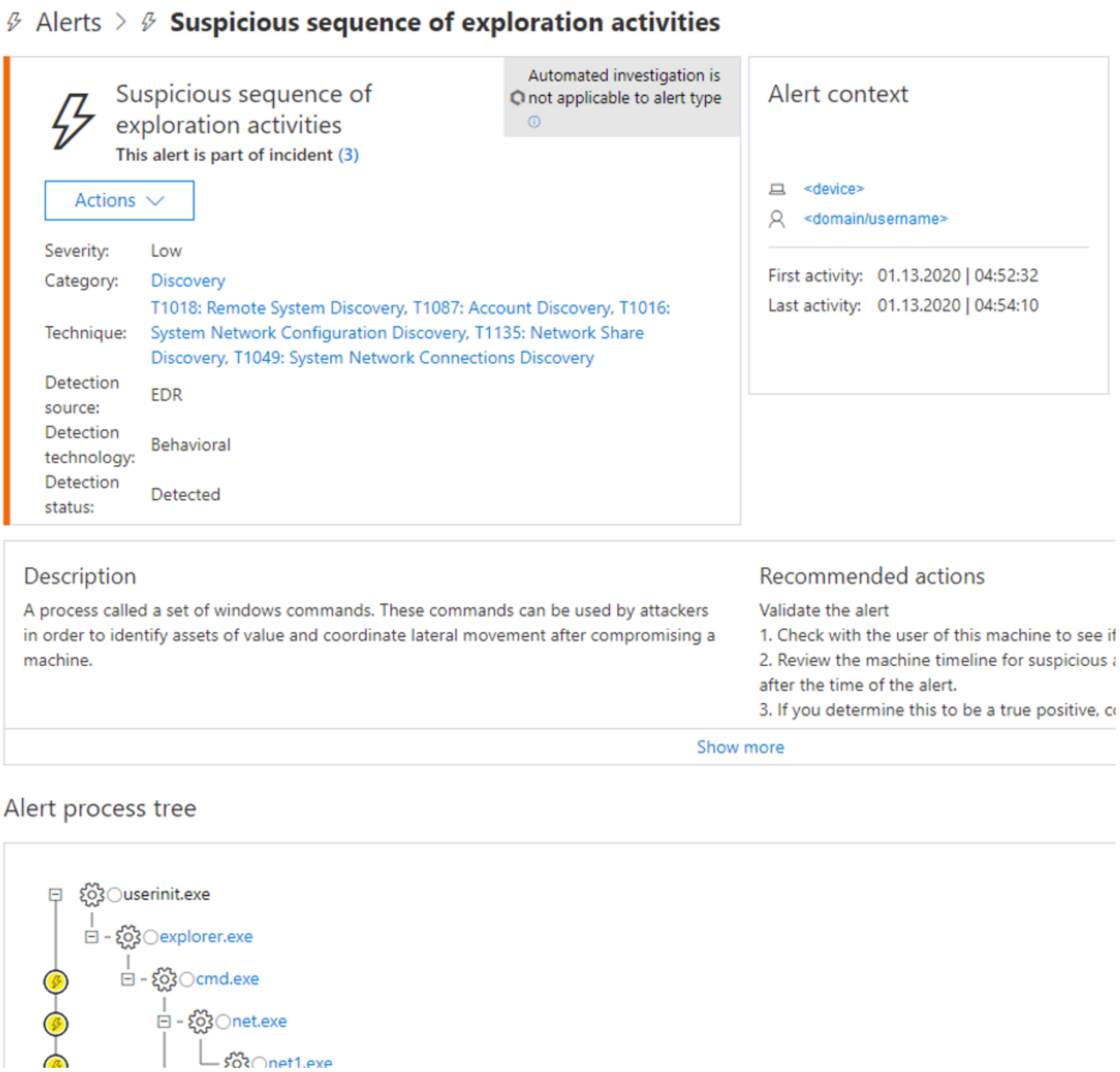
Recommendation Agency should ensure a recipient email address (typically the Agency cyber security team mailbox or similar) shared with multiple users is created and monitored.

The majority of alerts generated within the Microsoft 365 Defender portal – which include Microsoft Defender for Endpoint alerts – relate to automatically detected issues and are informational in nature. This means that they are not necessarily harmful to the system but must be reviewed and accounted for. Alerts are organised by severity as they enter the 'Alerts queue', the severity of which is detailed below in Table 2.

Table 2 Microsoft 365 Defender Alert Severities

Severity	Description
High	Threats marked as 'High' have the potential to cause severe damage to the system and devices using it. These alerts must be treated with urgency.
Medium	Threats marked as 'Medium' must be treated with some importance but typically will indicate anomalous behaviour within the environment such as the execution of suspicious files, un-sanctioned registry changes, or observed behaviours typical of a cyber threat or attack.
Low	'Low' urgency threats will typically be identified as commercial/known malware or hacking tools, their function is generally well understood and the ability to stop it is high.
Informational	'Informational' alerts are those that might not be considered harmful to the network but are good to track.

Figure 2 shows an example of an alert from Defender for Endpoint which detected a suspicious sequence of activities and automatically generated an incident detailing the severity, timestamps, devices affected, applications called, and more.


Alerts > Suspicious sequence of exploration activities

Suspicious sequence of exploration activities

This alert is part of incident (3)

Automated investigation is not applicable to alert type

Severity:	Low
Category:	Discovery
Technique:	T1018: Remote System Discovery, T1087: Account Discovery, T1016: System Network Configuration Discovery, T1135: Network Share Discovery, T1049: System Network Connections Discovery
Detection source:	EDR
Detection technology:	Behavioral
Detection status:	Detected

Alert context

<device>

<domain/username>

First activity: 01.13.2020 | 04:52:32

Last activity: 01.13.2020 | 04:54:10

Description

A process called a set of windows commands. These commands can be used by attackers in order to identify assets of value and coordinate lateral movement after compromising a machine.

Recommended actions

Validate the alert

1. Check with the user of this machine to see if

2. Review the machine timeline for suspicious a after the time of the alert.

3. If you determine this to be a true positive, co

Alert process tree

```
userinit.exe
  - explorer.exe
      - cmd.exe
          - net.exe
              └ net1.exe
```

Figure 2 Suspicious sequence of activities

When the Agency’s cyber security personnel receive an alert, they should perform analysis to determine the cause and any potential impact, including recommended actions within the Microsoft 365 Defender portal. If an alert occurs during an approved change window and relates directly to the contents of the change, for example an unapproved/not allowed executable runs during an application deployment, then it is unlikely that a security incident has occurred. However, if an alert is triggered outside of a change window and without an obvious cause then the probability of the event being a security incident probable.

Note, Microsoft assign a criticality to each alert based on an internal rating system. It is up to the Agency’s cyber security team to make their own assessment of the criticality of all potential security incidents in accordance with the Agency’s overarching IRP.

The assignment of criticality to an incident is an important step and due care must be applied to avoid the risks associated with both under and over classifying an incident. If there is ever any doubt, cyber security personnel should always investigate further.

The alerts captured in the Microsoft 365 Defender portal should be leveraged by Agency cyber security personnel to detect and analyse potential security incidents. The Microsoft 365 Defender portal provides far deeper detail than is available from the email alerts, these emails should only serve as a cursory notification, not an in-depth analysis of the incident.

Within the Microsoft 365 Defender portal there are two capabilities that should be utilised by Agency cyber security personnel for the purpose of detection and analysis of incidents on a day-to-day basis.

- Incidents lists all automatically generated incidents detected by Defender for Endpoint - along with Defender for Office 365 and Defender for Cloud Apps, including the severity of the incident, the machines and users involved, last activity, assignment of the incident, et cetera. All incidents should be assigned as they are generated and managed based on the Agency's operating procedures by cyber security personnel.
- Alerts queue lists all alerts based on the alert type not the incident case that is generated, this can be supremely helpful when attempting to identify patterns of behaviour. This alerts queue will also sort by severity, which incident it is related to, status, and investigation state.

For both the Incidents and Alerts queue Agency cyber security personnel can select individual records to access detailed information on the specific activity.

Incident criticality assignment Regardless of the detection source for a potential incident, all incidents should be assigned a criticality in a consistent manner. In accordance with guidance issued by the Agency's Chief Information Security Officer (CISO) or other personnel responsible for the daily operational information security of the Agency, all incidents should be assigned a system specific criticality. The criticality ratings for incidents have been developed from a number of Federal Government Agencies' overarching risk frameworks, specifically the consequence definitions. These definitions are listed below.

Note, if incident criticality definitions are included in the Agency IRP cyber security personnel should use those in preference to the criticalities defined below. The Business Impact Levels (BILs) defined in the Protective Security Policy Framework (PSPF) should also be considered in the assessment of incident criticalities.

Table 3 Incident Criticality Definitions

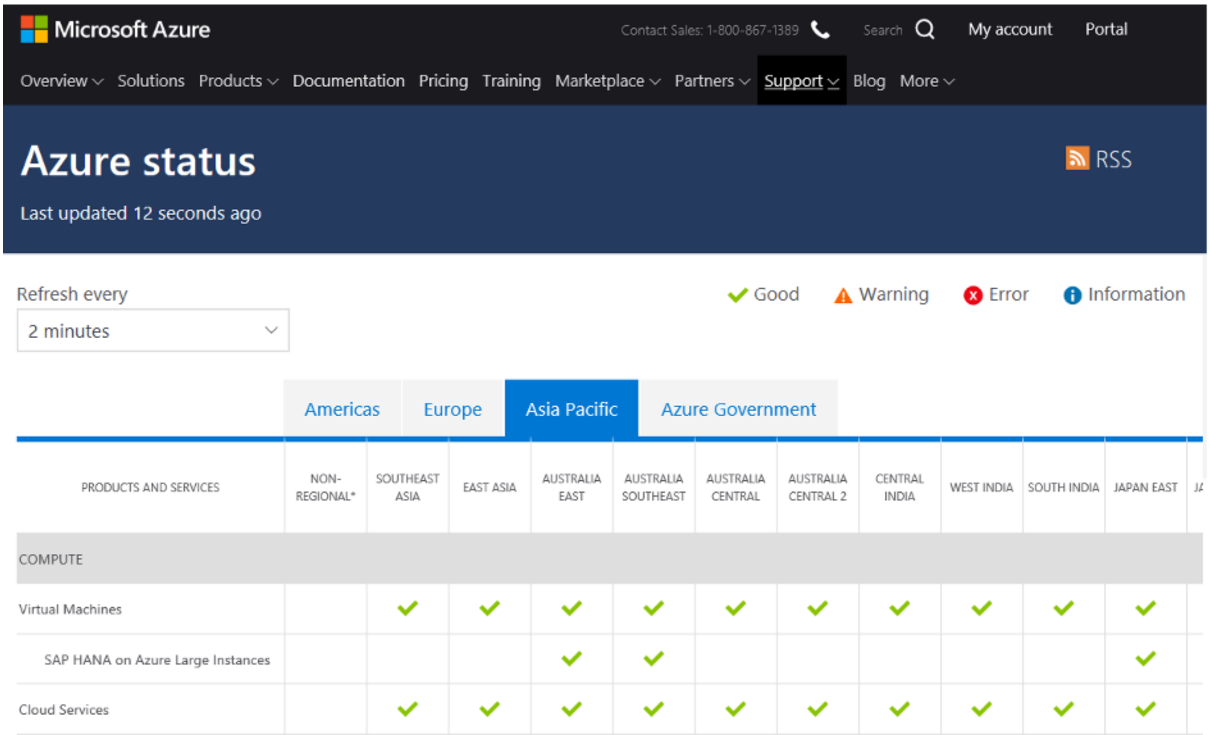
Incident Criticality	Performance Metrics	Reputational Metrics
Extreme	Major impact on departmental outcomes and performanceRequires major additional management effort by Senior Executive to control the impactUnavailability of agency mission critical systems including the delivery of Government outcomes (e.g. a public facing system that is used in emergency procedures, a grants systemCatastrophic breach and or loss and or destruction of agency information containing sensitive and personal information of Australian citizens and or classified information	Significant adverse publicityLoss of stakeholder confidence requiring intervention by SecretaryReporting to accountable authorities outside of the Agency e.g. Privacy Commissioner, Minister of Department etc
High	Moderate impact on achievement of outcomes and performanceRequires additional management effort by business area, Senior Executive to control the impact	Substantial adverse publicityLoss of stakeholder confidence requiring intervention at Executive level
Medium	Minor impact on achievement of outcomes and performanceRequires additional management effort within the business area to control the impact	Some adverse publicityMinor loss of stakeholder confidence

Incident Criticality	Performance Metrics	Reputational Metrics
Low	Insignificant impact on achievement of outcomes and performance	Some adverse publicityMinor loss of stakeholder confidence

Agency cyber security personnel should use the above table to define the criticality of incidents based on the data available to them at the time of detection and analysis. If this data is updated or found to be inaccurate Agency cyber security personnel should re-assess the criticality of the related incident(s). The criticality of an incident should be used to determine the resources, timeframes and reporting requirements related to it.

Azure service outages An additional data source that can be leveraged by Agency cyber security personnel when analysing potential security incidents is the Azure status dashboard. This dashboard is published by Microsoft and reports on the current status of all Azure-based services, including any current warnings or errors. An example of the dashboard is shown below in Figure 3.

The Azure status dashboard is available at https://status.azure.com/ and does not require the user to be logged into Azure to view the current status.



Azure status

Last updated 12 seconds ago

PRODUCTS AND SERVICES	NON-REGIONAL*	SOUTHEAST ASIA	EAST ASIA	AUSTRALIA EAST	AUSTRALIA SOUTHEAST	AUSTRALIA CENTRAL	AUSTRALIA CENTRAL 2	CENTRAL INDIA	WEST INDIA	SOUTH INDIA	JAPAN EAST	JA
COMPUTE												
Virtual Machines		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
SAP HANA on Azure Large Instances				✓	✓						✓	
Cloud Services		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	

Figure 3 Azure Status Dashboard

Agency cyber security personnel can use the dashboard to determine if a potential incident is local to the Agency's system or is a widespread issue affecting the underlying Azure service(s).

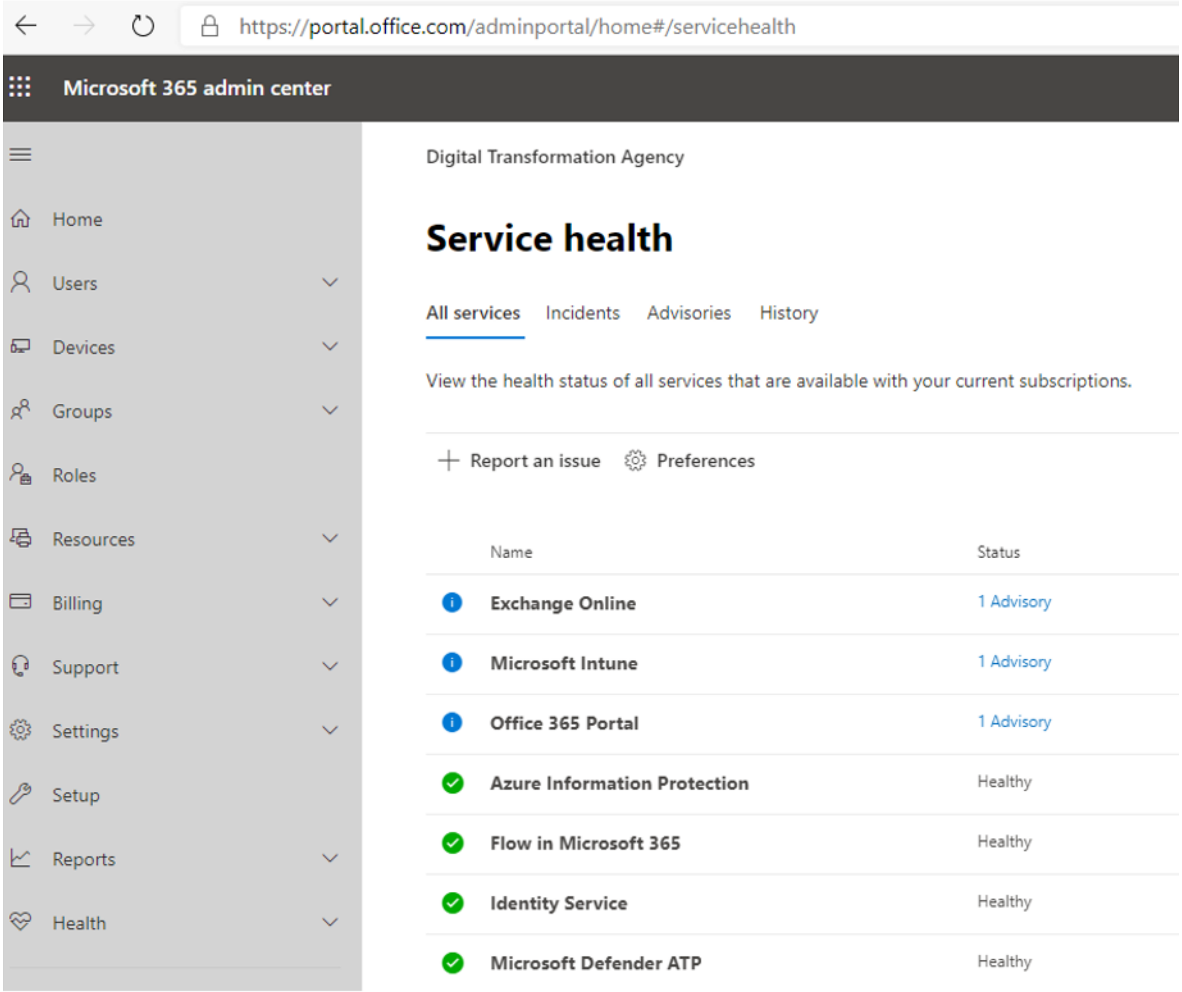
Recommendation It is recommended that at least one Agency cyber security personnel member is subscribed to the provided Rich Site Summary (RSS) feed to receive updates whenever an Agency-leveraged service is affected.

Microsoft 365 service outages Agency cyber security personnel should review the Microsoft 365 service status (including all Office 365 services) when investigating an incident relating to availability. The following resources are available from Microsoft to identify the status of Microsoft 365 services:

- Microsoft 365 Service health status
- Microsoft 365 Status Twitter

In the first instance the Microsoft 365 Service health status page should be consulted, followed by the Microsoft 365 Status Twitter account. If no issues are identified by either of these resources, then Agency-specific scenarios should be explored such as loss of Internet connect, Local Area Network (LAN) outage, etc.

As an example of how to navigate the Microsoft 365 Service health status page, please refer to Figure 4 below.



Digital Transformation Agency

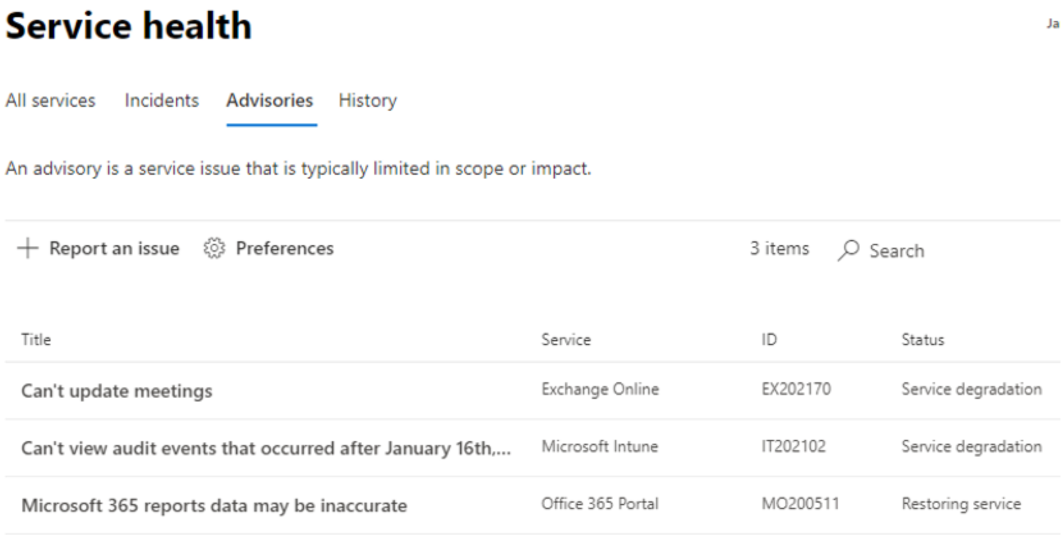
Service health

View the health status of all services that are available with your current subscriptions.

Name	Status
Exchange Online	1 Advisory
Microsoft Intune	1 Advisory
Office 365 Portal	1 Advisory
Azure Information Protection	Healthy
Flow in Microsoft 365	Healthy
Identity Service	Healthy
Microsoft Defender ATP	Healthy

Figure 4 Office 365 Service Outages

Agency cyber security personnel can use the dashboard to determine if a service is down, whether the issue is widespread and affecting the underlying services, or whether there is no identified outage. This page can also be used to review ongoing service advisories such as those identified below in Figure 5.



Service health

An advisory is a service issue that is typically limited in scope or impact.

Title	Service	ID	Status
Can't update meetings	Exchange Online	EX202170	Service degradation
Can't view audit events that occurred after January 16th,...	Microsoft Intune	IT202102	Service degradation
Microsoft 365 reports data may be inaccurate	Office 365 Portal	MO200511	Restoring service

Figure 5 Office 365 Service Health Advisories

Recommendation It is recommended that at least one Agency cyber security team member, or another person assigned with cyber security responsibilities, review these services daily to ensure there are no ongoing service outages that will affect the availability.

Containment, eradication, and recovery

The Agencies cyber security teams' approach to containment, eradication, and recovery – particularly in relation to resource allocation and priority – should be based on the category of the incident as previously described. However, regardless of the criticality of an incident the basic actions that are required to address the incident are dependent on the specific incident type.

This IRP defines specific incident types that are directly related to the solution, namely:

- Violation of confidentiality of Agency data stored in Office 365 (including Exchange Online)
- Violation of integrity and/or confidentiality of Azure AD accounts
- Violation of integrity of Azure AD configuration
- Violation of integrity of Office 365 configuration
- Loss of availability of Agency data stored in Office 365

The following table provides recommendations for the containment, eradication, and recovery activities associated with the above incident types:

Table 4 Incident Containment, Eradication, and Recovery Activities

Incident type	Containment, Eradication, and Recovery Activities
Violation of confidentiality of Agency data stored in Office 365(For example, sensitive information is sent outside the organisational boundaries – data spill)	**Containment** – Data Loss Prevention (DLP) policies are in place across Microsoft Teams, Exchange Online, SharePoint Online, and Outlook. All data stored in these corporate data locations is backed by policies to block the egress of what is identified as 'sensitive'. Note, if DLP policies have been disabled or modified they should be re-enabled and verified by referring to the relevant ABAC.**Eradication** – DLP policies automatically block messages from being sent or redacts and obfuscates data attempting to leave organisational boundaries.**Recovery** – Recovery of sensitive information is automated by DLP. User notifications are linked to DLP policies upon creation. The Agency cyber security team should review DLP policies often to ensure they align with business needs. New policies should be created based on commonly used applications within the organisation.
Violation of integrity and/or confidentiality of Azure AD account(s)(For example, user or administrative account compromised)	**Containment** – Compromised account credentials can result in catastrophic damage to the system if the account in question has administrative privileges, and breaches of sensitive data. To contain this, Conditional Access and Multi-Factor Authentication (MFA) are employed to control access to all accounts, even if account credentials are compromised. Agency cyber security personnel can perform a global account sign-out and password reset if an account is suspected of being compromised.**Eradication** – Compromised accounts can be disabled from log-ins, passwords reset, and global sign-outs initiated. Agency cyber security personnel should review Azure AD logs to identify the source of the breach from an identity perspective. They should also review sharing audit logs against SharePoint Online and OneDrive for Business prior to the user being given their account credentials back. Additionally, a full audit of the user's log-in habits should be performed to ensure they comply with Agency security requirements.**Recovery** – Once the incident has been remediated the users account should be re-enabled, password reset, and access granted. Simultaneous to this, the Agency cyber security team are to review all appropriate logs dependant on the breach.

Incident type	Containment, Eradication, and Recovery Activities
Violation of integrity of Azure AD configuration(For example, unapproved changes are made to Conditional Access policies)	**Containment** – Unauthorised changes to Conditional Access policies can result in gaps within the approved authentication process. To prevent these changes Privileged Identity Management should be utilised to only grant temporary permissions to perform privileged tasks.**Eradication** – Agency cyber security personnel should revert any changes made to the configuration in alignment with the configuration outlined in the 'DTA – Platform – Detailed Design' and 'DTA – Conditional Access – ABAC' documents.**Recovery** – Ensure all changes have been reverted, to ensure this has been completed successfully refer to the design and ABAC documents. Once the change(s) have been reverted any further authentication attempts will need to pass the conditional access policies. Measures should be in place to record any security incidents and unexpected changes to the configuration due to lack of knowledge.
Violation of integrity of Office 365 configuration(For example, DLP or retention policies are disabled or modified without authorisation)	**Containment** – DLP and retention policies are in place to ensure sensitive data does not improperly leave organisational boundaries. DLP is controlled by Azure AD permissions, as such, all access to it should be controlled by Privileged Identity Management (PIM). In the event of an incident PIM can be used to restrict administrative privileges to prevent further changes and provide an audit log of previous actions.**Eradication** – Agency cyber security personnel should revert any changes made to the configuration in alignment with the configuration in the 'DTA – Office 365 – Detailed Design' document. The Azure AD and PIM logs should be scrutinised to review by whom the unapproved change was made.**Recovery** – Ensure all changes have been reverted, to ensure this has been completed successfully refer to the design and ABAC documents. Agency cyber security personnel should review the last modified time of the affected policy and align it with PIM logs. A review of all privileged users and groups is recommended.

Incident type	Containment, Eradication, and Recovery Activities
Loss of availability of Agency data stored in Office 365(For example, the Microsoft Teams service is unavailable, and critical corporate data cannot be accessed)	**Containment** – Service availability within the Office 365 and Azure environments is very high, if however, a service is offline or otherwise inaccessible, the Agency cyber security team should ensure the status of the service via the Microsoft 365 Service Health Status portal (see: Microsoft 365 Service Outages). If Microsoft Teams is inaccessible, secondary pathways to the data should be explored, for example, accessing the Teams back-end SharePoint Online site.**Eradication** – Not applicable for availability incidents.**Recovery** – The service is controlled by Microsoft and its availability is backed by Microsoft service level agreements.

Note, the activities listed above are designed to aid Agency cyber security personnel in responding to the specific incident types defined. However, this is not an exhaustive list of all possible responses. Agency cyber security personnel should use their judgement to determine if they are appropriate to a specific incident or if other actions should be taken.

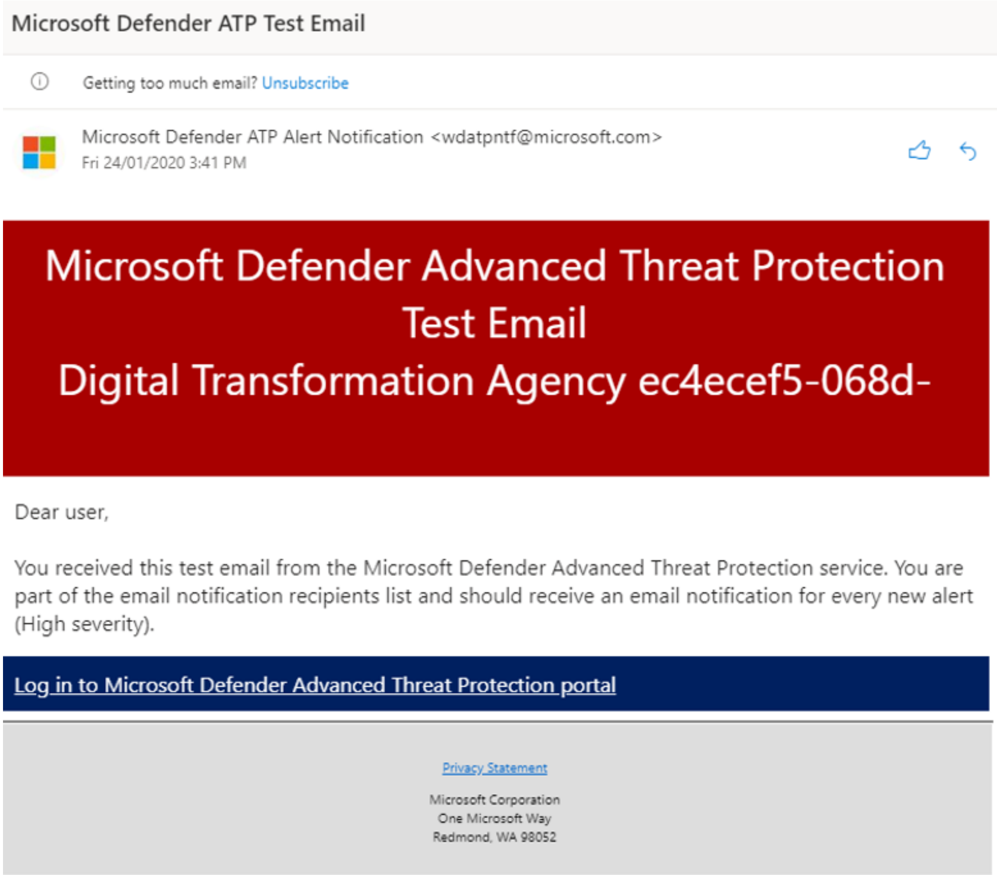
Defender for Endpoint threat remediation Defender for Endpoint provides the ability to automate responses to detected threats, reducing the total response time for an incident and eliminating the need for manual actions to be taken by the Agency's cyber security team. Five levels of automation are available as listed below:

- No automated response – automated investigations are not run, and all activities must be performed by the Agency's cyber security team.
- Semi (any folder) – approval is required from the cyber security team for all remediation activities suggested as part of an automated investigation.
- Semi (non-temp folders) – remediation occurs automatically for temporary folders including users' download folders, remediation for other locations requires approval.
- Semi (core folders) – remediation occurs automatically for all folders other than operating system directories (e.g. Program Files and Window).
- Full – all remediation activities are performed automatically.

The CloudSystem uses the default Defender for Endpoint configuration for automated investigations, namely Full automation. Therefore, Agency cyber security personnel will not be prompted to approve remediation activities that are recommended as part of Defender for Endpoint automated investigations. The automation level can be adjusted if required based on the specific requirements of the Agency's cyber security personnel.

Note, prior to early 2021, the default configuration was Semi (any folder).

Automated remediation notification Depending on the nature of the initial alert, if Microsoft Defender for Endpoint detects a threat and it is resolved automatically it will notify administrators by sending a follow up email. An example of an alert resolution email is shown below in Figure 6.



Microsoft Defender ATP Test Email

Getting too much email? Unsubscribe

Microsoft Defender ATP Alert Notification <wdatpntf@microsoft.com>
Fri 24/01/2020 3:41 PM

Microsoft Defender Advanced Threat Protection Test Email
Digital Transformation Agency ec4ecef5-068d-

Dear user,

You received this test email from the Microsoft Defender Advanced Threat Protection service. You are part of the email notification recipients list and should receive an email notification for every new alert (High severity).

Log in to Microsoft Defender Advanced Threat Protection portal

Privacy Statement

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

Figure 6 Alert Resolution Email

Agency cyber security personnel should be aware of these notifications but should not rely on them as a trigger to cease investigation and/or recovery activities.

Recommendation It is recommended that Agency cyber security personnel verify that an incident resulting from alert is actually resolved before moving to the post-incident phase.

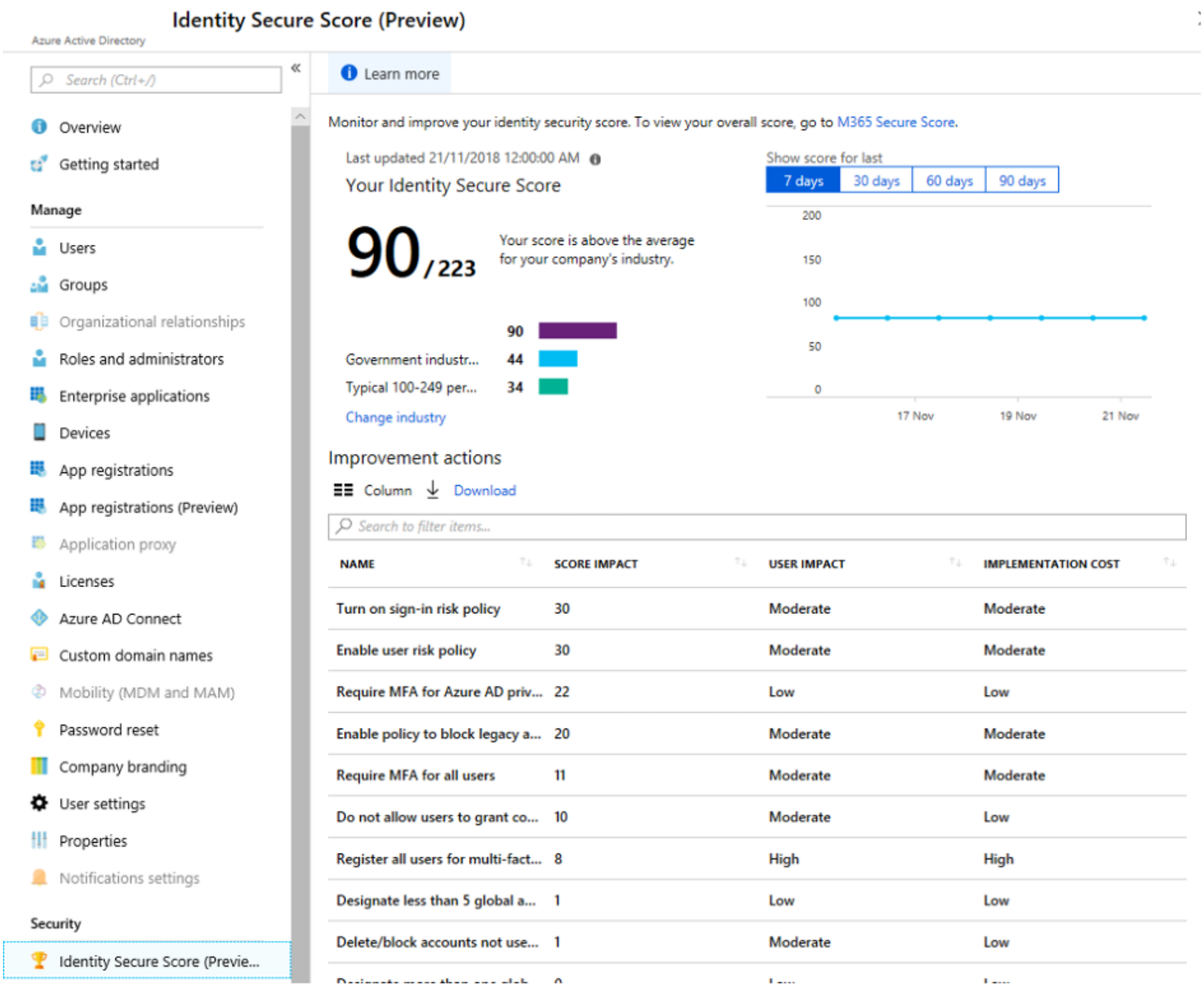
Post-incident activity

In accordance with the Agency's overarching IRP recommendation, 'lessons learnt' meetings should be held after all major incidents. However, for incidents it is recommended that one of these meetings is held after every incident. This provides an opportunity to assess the current controls in place and evaluate if additional controls can be applied to prevent or minimise the effect of a similar incident occurring again.

Due to the regular update cadence for Azure and Office 365, new features are made available monthly. This often includes Preview features in Azure that provide enhanced capabilities but are still under development by Microsoft. One of the goals of the post-incident meetings should be to assess newly released and preview features for their potential to reduce the risk of the incident re-occurring. This may require specialist resources to attend to present newly available features and discuss how implementing them may reduce the risk to the system.

Note, new capabilities and services – including all Preview features – should be assessed by Agency cyber security personnel before being enabled.

Figure 7 illustrates how a preview feature is presented in the Azure portal using the "… (Preview)" suffix to the feature/service name.



Monitor and improve your identity security score. To view your overall score, go to M365 Secure Score.

Last updated 21/11/2018 12:00:00 AM

Your Identity Secure Score

90 / 223

Your score is above the average for your company's industry.

	90
Government industr...	44
Typical 100-249 per...	34

Improvement actions

NAME	SCORE IMPACT	USER IMPACT	IMPLEMENTATION COST
Turn on sign-in risk policy	30	Moderate	Moderate
Enable user risk policy	30	Moderate	Moderate
Require MFA for Azure AD priv...	22	Low	Low
Enable policy to block legacy a...	20	Moderate	Moderate
Require MFA for all users	11	Moderate	Moderate
Do not allow users to grant co...	10	Moderate	Low
Register all users for multi-fact...	8	High	High
Designate less than 5 global a...	1	Low	Low
Delete/block accounts not use...	1	Moderate	Low
Designate more than one glob...	0	Low	Low

Figure 7 Azure AD Preview Feature

Note, as of the time of writing the Azure AD Identity Secure Score feature is no longer in preview and is generally available for all tenants.

The outcomes of all post-incident meetings should be recorded in the report prepared for each incident. This ensures there is a document chain of events for the incident including tasks that will now be undertaken due to the analysis of the incident, but potentially not directly related (for example applying an additional control to prevent a future incident). This report may be the subject of an internal or external audit in accordance with the Agencies reporting requirements and therefore should be treated as a formally controlled document and stored in accordance with existing policies. Additionally, any information collected as part of the incident response should be either be directly included in the report, or its storage location referenced, as applicable.

All other aspects of the 'lessons learnt' meetings and reporting requirements should be undertaken in accordance with the recommendations provided in the Agency's overarching IRP.

Coordination with external resources

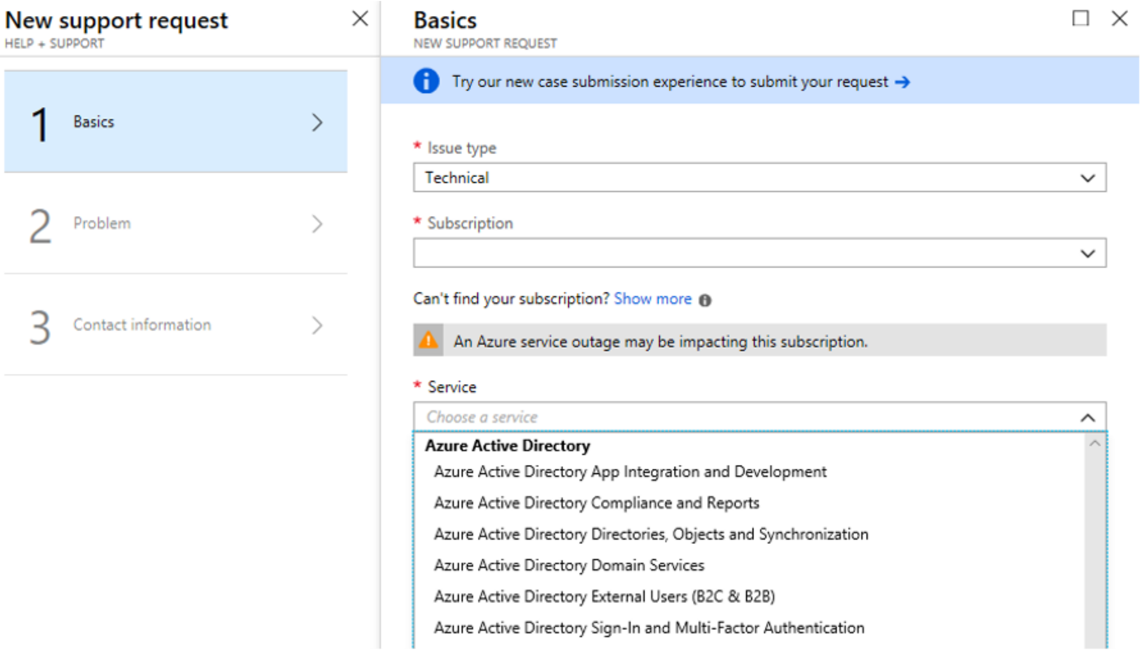
In some cases, Agency cyber security personnel may require the assistance of additional external resources to aid in one or more phases of the Incident Response Life Cycle. When this is required, Agency cyber security personnel should follow existing Agency policies and procedures to appropriately engage and communicate with external resources to assist with incident management and response.

Microsoft support requests

With the introduction of Azure AD an additional external resource becomes available to assist Agency cyber security personnel manage and respond to security incidents. Microsoft Support Requests can be made from within the Azure Portal to report issues and access assistance with all Azure hosted services, including Azure AD, Azure MFA, and Conditional Access. Support Requests are associated with Azure Subscriptions, and a user must have 'write permissions' for the subscription to raise a support request.

The New support request wizard provides a three-step process to detail and submit new support requests via the Azure Portal. The three steps are:

- Basics – which includes the issue type (most likely to be technical if raised in relation to a security incident), the subscription affected and the specific service. This is illustrated below in Figure 8.
- Problem – which includes a technical description of the issue/incident including severity, problem type, category, title, and details. It also provides fields to identify when the problem started and provide the option for the user to upload a file.
- Contact information – which includes contact details for a Microsoft engineer to use to assist with the support request. Depending on the reported severity of the issue the Preferred contact method and Response may be auto-filled (for example, high severity requests default to phone and 24x7 respectively).



New support request
HELP + SUPPORT

1 Basics

2 Problem

3 Contact information

Basics
NEW SUPPORT REQUEST

Try our new case submission experience to submit your request →

* Issue type: Technical

* Subscription:

Can't find your subscription? Show more

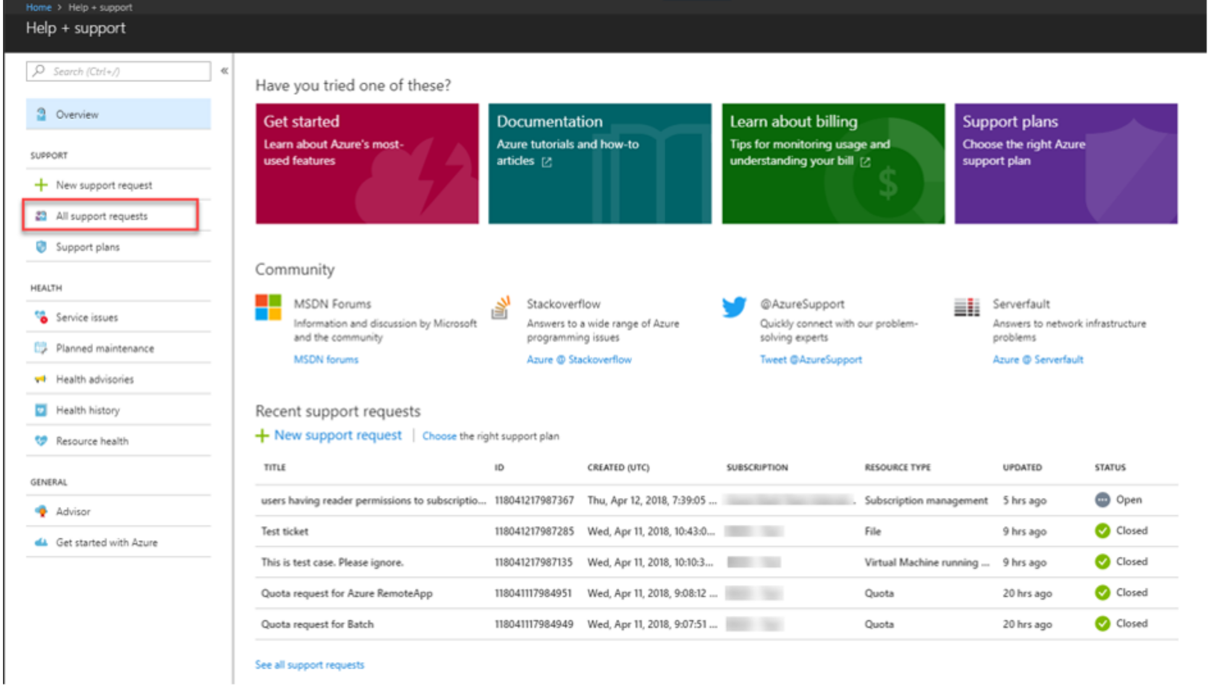
An Azure service outage may be impacting this subscription.

* Service: Choose a service

Azure Active Directory
Azure Active Directory App Integration and Development
Azure Active Directory Compliance and Reports
Azure Active Directory Directories, Objects and Synchronization
Azure Active Directory Domain Services
Azure Active Directory External Users (B2C & B2B)
Azure Active Directory Sign-In and Multi-Factor Authentication

Figure 8 New Support Request

The progress of support requests can also be tracked from within the Azure Portal under the Help + support page. This is illustrated below in Figure 9.



Have you tried one of these?

Get started
Learn about Azure's most-used features

Documentation
Azure tutorials and how-to articles

Learn about billing
Tips for monitoring usage and understanding your bill

Support plans
Choose the right Azure support plan

Community

MSDN Forums
Information and discussion by Microsoft and the community
MSDN forums

Stackoverflow
Answers to a wide range of Azure programming issues
Azure @ Stackoverflow

@AzureSupport
Quickly connect with our problem-solving experts
Tweet @AzureSupport

Serverfault
Answers to network infrastructure problems
Azure @ Serverfault

Recent support requests

+ New support request | Choose the right support plan

TITLE	ID	CREATED (UTC)	SUBSCRIPTION	RESOURCE TYPE	UPDATED	STATUS
users having reader permissions to subscriptio...	118041217987367	Thu, Apr 12, 2018, 7:39:05 ...	[redacted]	Subscription management	5 hrs ago	Open
Test ticket	118041217987285	Wed, Apr 11, 2018, 10:43:0...	[redacted]	File	9 hrs ago	✓ Closed
This is test case. Please ignore.	118041217987135	Wed, Apr 11, 2018, 10:10:3...	[redacted]	Virtual Machine running ...	9 hrs ago	✓ Closed
Quota request for Azure RemoteApp	118041117984951	Wed, Apr 11, 2018, 9:08:12 ...	[redacted]	Quota	20 hrs ago	✓ Closed
Quota request for Batch	118041117984949	Wed, Apr 11, 2018, 9:07:51 ...	[redacted]	Quota	20 hrs ago	✓ Closed

See all support requests

Figure 9 All Support Requests

For more information on creating Azure support requests, including any updates to the process, refer to Create an Azure support request.

Australian Cyber Security Centre

In the case where an incident has not been able to be resolved using the steps defined previously, the ACSC may be engaged by agency approved staff as per the Agency’s overarching IRP.

An incident can be reported to the ACSC via the following methods:

- Website - https://www.cyber.gov.au/contact
- Phone number – 1300 CYBER1 (1300 292 371)
- Email – asd.assist@defence.gov.au

Note, reporting an incident via the phone is preferred when the incident is considered urgent by the Agency.

Document Control

Title	Malware Playbook
Version	2.3
Date Issued	20/01/2020
Status	Draft
Document owner	Scottish Government
Creator name	
Creator organisation name	NCC Group
Subject category	Cyber Incident Response Management
Access constraints	

Document Revision History

Version	Date	Author	Summary of changes
2.3	22/01/2020	SG CRU	Generic Version Created from Public Sector Playbook

Contents

1. Introduction

2. 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.

3. 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.

4. 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.

5. 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.

6. 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.

7. 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>>; (insert Links) • <<Data Flow Diagrams>>.(insert Links)	• 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; • Reporting a suspected cyber incident.	• Head of IT • Information Security Manager • Resilience Lead • Business Continuity Lead
	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

8. 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. Consider reporting to Police Scotland where criminal Investigation may be warranted	• Information Security Manager • Core IT CIRT
	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	• Information Security Manager • Core IT CIRT • CIRT

	Scotland	
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

9. Analyse

Analysis Phase		
bjectives	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.	
tivity	**Description**	**Stakeholders**
the extent ncident	Activities may include, but are not limited to:	
	Engage technical staff from resolver groups.	- Service Desk Technici - Core IT CIRT
	Classify the malware by submission to multiple AV vendors and determine the family it belongs to.	- Information Security M - 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 M • Core IT CIRT • CIRT
	Reverse-engineer the malware in a secure environment to understand its mechanisms, and the functionality it implements.	• Information Security M • 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 M • Core IT CIRT
	Review affected infrastructure for indicators of compromise derived from the malware analysis to identify any additional compromised system(s).	• Information Security M • Core IT CIRT
	Preserve all evidence to support attribution or anticipated legal action.	• Information Security M • 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 M • Core IT CIRT
	Verify all infected assets are in the process of being recalled and quarantined.	• Information Security M • Core IT CIRT • CIRT

10. Remediation – Contain, Eradicate and Recover

	Remediation Phase	
bjectives	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.	
ctivity	Description	Stakeholde
ment	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 M • Core IT CIRT
	Ensure that the latest malware definitions have been deployed across the anti-malware solution.	• Information Security M • Core IT CIRT
	Initiate an estate-wide anti-malware scan.	• Information Security M • 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: • 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.	• Information Security M • Core IT CIRT
	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 M • Core IT CIRT • CIRT
	Suspend the login credentials of suspected compromised accounts.	• Information Security M • 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 M • Core IT CIRT
	Inform business data owner(s) and stakeholders of the progress of containment activities.	• Information Security M • CIRT • Resilience Lead • Business Continuity L • Policy Area Lead
ctivity	Description	Stakeholde
ion	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 M • Core IT CIRT

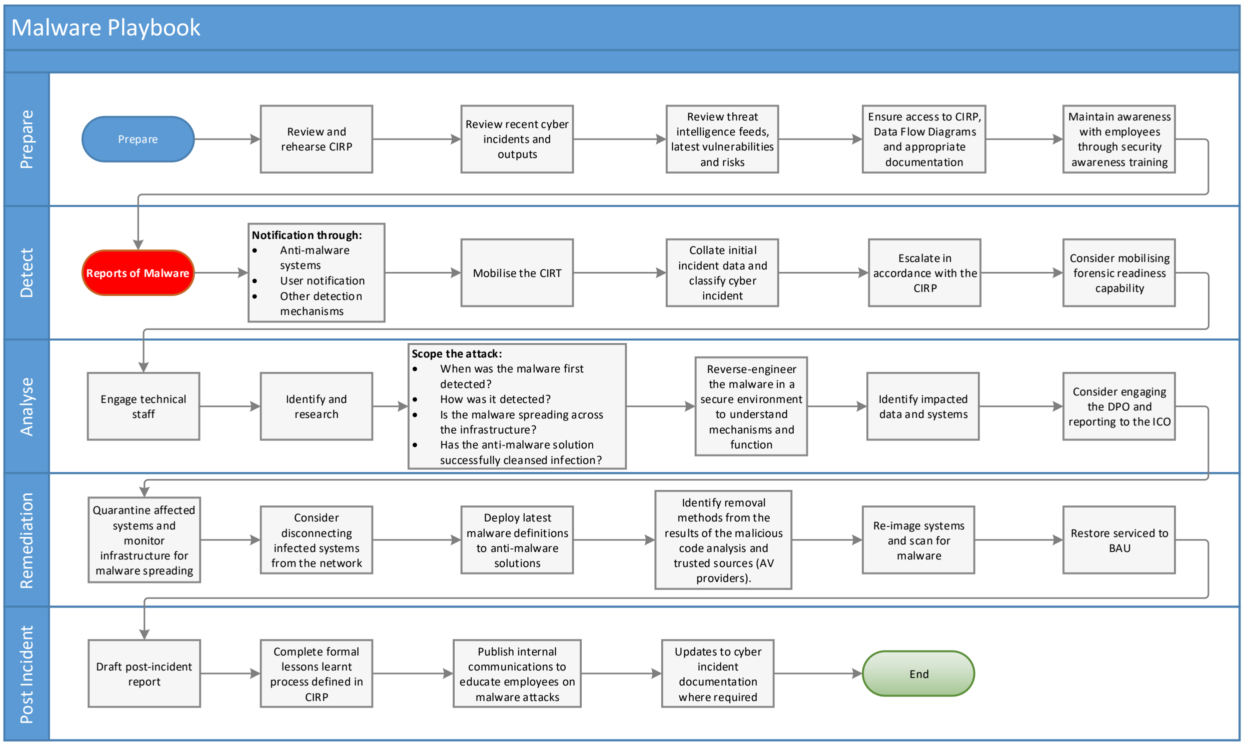
	Complete an automated or manual removal process to eradicate malware or compromised executables using appropriate tools.	• Information Security M • Core IT CIRT
	Conduct a restoration of affected networked systems from a trusted back up.	• Information Security M • Core IT CIRT
	Re-install any standalone systems from a clean OS back-up before updating with trusted data back-ups.	• Information Security M • Core IT CIRT
	Change any compromised account details.	• Information Security M • Core IT CIRT
	Continue to monitor for signatures and other indicators of compromise to prevent the malware attack from re-emerging.	• Information Security M • Core IT CIRT
	Confirm policy compliance across the estate.	• Information Security M • Core IT CIRT

ctivity	Description	Stakeholde
to BAU	Activities may include, but are not limited to:	
	Recover systems based on business impact analysis and business criticality.	• Information Security M • Core IT CIRT
	Complete malware scanning of all systems, across the estate.	• Information Security M • Core IT CIRT
	Re-image systems.	• Information Security M • Core IT CIRT
	Re-set the credentials of all involved system(s) and users account details.	• Information Security M • Core IT CIRT
	Reintegrate previously compromised systems.	• Information Security M • Core IT CIRT
	Restore any corrupted or destroyed data.	• Information Security M • Core IT CIRT
	Restore any suspended services.	• Information Security M • Core IT CIRT
	Establish monitoring to detect further suspicious activity.	• Information Security M • Core IT CIRT
	Co-ordinate the implementation of any necessary patches or vulnerability remediation activities.	• Information Security M • Core IT CIRT

11. Post Incident

	Post-Incident Activities Phase	
jectives	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.	
ctivity	Description	Stakeholde
t 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 M
Identified em ment	Complete the formal lessons identified process to feedback into future preparation activities.	• Information Security M • CIRT • Resilience Lead
	Consider sharing lessons identified with the wider stakeholders where relevant	• Information Security M • CIRT • Resilience Lead • Business Continuity L
	Conduct root cause analysis to identify and remediate underlying vulnerabilities.	• Information Security M • CIRT
Resources	Review staff welfare; working hours, over time, time off in lieu (TOIL) and expenses.	• Information Security M • HR
nications	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 M • CIRT • Communications • Resilience Lead • Business Continuity L
	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 M • Communications Tear

12. Annex A: Flow Diagram


Malware Playbook
Prepare
Prepare
Review and rehearse CIRP
Review recent cyber incidents and outputs
Review threat intelligence feeds, latest vulnerabilities and risks
Ensure access to CIRP, Data Flow Diagrams and appropriate documentation
Maintain awareness with employees through security awareness training
Detect
Reports of Malware
Notification through:
Anti-malware systems
User notification
Other detection mechanisms
Mobilise the CIRT
Collate initial incident data and classify cyber incident
Escalate in accordance with the CIRP
Consider mobilising forensic readiness capability
Analyse
Engage technical staff
Identify and research
Scope the attack:
When was the malware first detected?
How was it detected?
Is the malware spreading across the infrastructure?
Has the anti-malware solution successfully cleansed infection?
Reverse-engineer the malware in a secure environment to understand mechanisms and function
Identify impacted data and systems
Consider engaging the DPO and reporting to the ICO
Remediation
Quarantine affected systems and monitor infrastructure for malware spreading
Consider disconnecting infected systems from the network
Deploy latest malware definitions to anti-malware solutions
Identify removal methods from the results of the malicious code analysis and trusted sources (AV providers).
Re-image systems and scan for malware
Restore serviced to BAU
Post Incident
Draft post-incident report
Complete formal lessons learnt process defined in CIRP
Publish internal communications to educate employees on malware attacks
Updates to cyber incident documentation where required
End

Malware Incident Response Plan03:

Preparation

Note: Preparation steps should primarily be completed prior to an event or incident. If the playbook is being accessed during an event or incident you may proceed to Preparation Step 4b.

1. Determine the members of the Cybersecurity Incident Response Team (CSIRT).
    1. The core CSIRT members should be comprised of individuals responsible for cybersecurity only.
        1. This may include some members of Information Technology roles, depending on the organization size.
        2. The limited size of the core CSIRT is to assist with confidentiality and efficiency.
        3. The core CSIRT may be activated often to investigate security events that may or may not result in an incident.
    2. Assign roles and responsibilities to each member.
2. Determine extended CSIRT members.
    1. This will often be Legal, Compliance, Public Relations, and Executive Leadership.
3. Define escalation paths.
    1. Incidents may start as events, or as a lower impact/severity and then increase as more information is gathered. Establishing an escalation path is critical to success.
4. Evaluate and secure critical system backups.
    1. Backups should be secured prior to any incident.
    2. During the initial stages of any incident, evaluate and confirm that backups are secure and not impacted by the incident.

Identification

1. Isolate infected systems ASAP.
    1. DO NOT power off machines, as forensic artifacts may be lost.
    2. Preserve the system(s) for further forensic investigation including log review, MFT analysis, deep malware scans, etc.
        1. These steps should be performed during the Identification phase to guide the investigation.
2. Investigate malware to determine if it’s running under a user context.
    1. If so, disable this account (or accounts if multiple are in use) until the investigation is complete.
3. Analyze the malware to determine characteristics that may be used to contain the outbreak.
    1. If available, use a sandboxed malware analysis system to perform analysis.
        1. **Note:** Network connectivity should not be present for this sandbox system except in very rare circumstances. Network activity from malware may be used to alert an attacker of your investigation.
        2. Observe any attempts at network connectivity, note these as Indicators of Compromise (IoCs)
        3. Observe any files created or modified by the malware, note these as IoCs.
        4. Note where the malware was located on the infected system, note this as an IoC.
        5. Preserve a copy of the malware file(s) in a password protected zip file.
    2. Use the PowerShell “Get-FileHash” cmdlet to get the SHA-256 hash value of the malware file(s).
        1. This hash may also be used to search for community information regarding this malware (i.e. VirusTotal, Hybrid-Analysis, CISCO Talos, etc.)
        2. Additional hash values (SHA1, MD5, etc.) may be gathered to better suit your security tools.
        3. Note these hash values as IoCs.

        3. Use all IoCs discovered to search any available tools in the environment to locate additional infected hosts.
4. Use all information and IoCs available to determine if the malware is associated with further attacks.
    1. i.e. Emotet, Trickbot, and Qakbot are often involved in Ryuk ransomware attacks.
    2. If further attacks are associated, gather all additional information available on these attacks to further the investigation.
5. Use all information and IoCs available to search for the initial point of entry.
    1. Determine the first appearance of the malware.
    2. Determine the user first impacted by the malware.
    3. Investigate all available log files to determine the initial date and point of infection.
    4. Analyze all possible vectors for infection.
        1. Focus on known delivery methods discovered during malware analysis (email, PDF, website, packaged software, etc.).

Containment

1. Use the information about the initial point of entry gathered in the previous phase to close any possible gaps.
    1. Examples: Firewall configuration changes, email blocking rules, user education, etc.
2. Once the IoCs discovered in the Identification phase have been used to find any additional hosts that may be infected, isolate these devices as well.
3. Add IoCs (such as hash value) to endpoint protection.
    1. Set to block and alert upon detection.
4. Submit hash value to community sources to aid in future detection.
    1. **NOTE:** Clear this process with legal/compliance representatives during each incident, as each malware situation will be different.
5. If additional further attacks were noted as associated with the malware, use IoCs and threat-intel to apply additional controls to prevent the attack from escalating.
6. Implement any temporary network rules, procedures and segmentation required to contain the malware.
7. If additional accounts have been discovered to be involved or compromised, disable those accounts.

Eradication

1. Preserve artifacts, systems, and relevant backups according to the sensitivity and scale of the incident. These may be important for future forensics.
    1. If rebuilding or replacing physical systems, preserve physical hard disks, solid state drives, or forensically sound images of those storage drives.
    2. If rebuilding or replacing virtual machines, preserve a copy, full (independent) snapshot, or a backup of the system.
2. Preserve any volatile data that may have been collected during the identification and containment phases.
    1. This may include log files, backups, malware samples, memory images, etc.
3. Once all relevant data, equipment, and/or systems have been preserved, replace, or rebuild systems accordingly.

Recovery

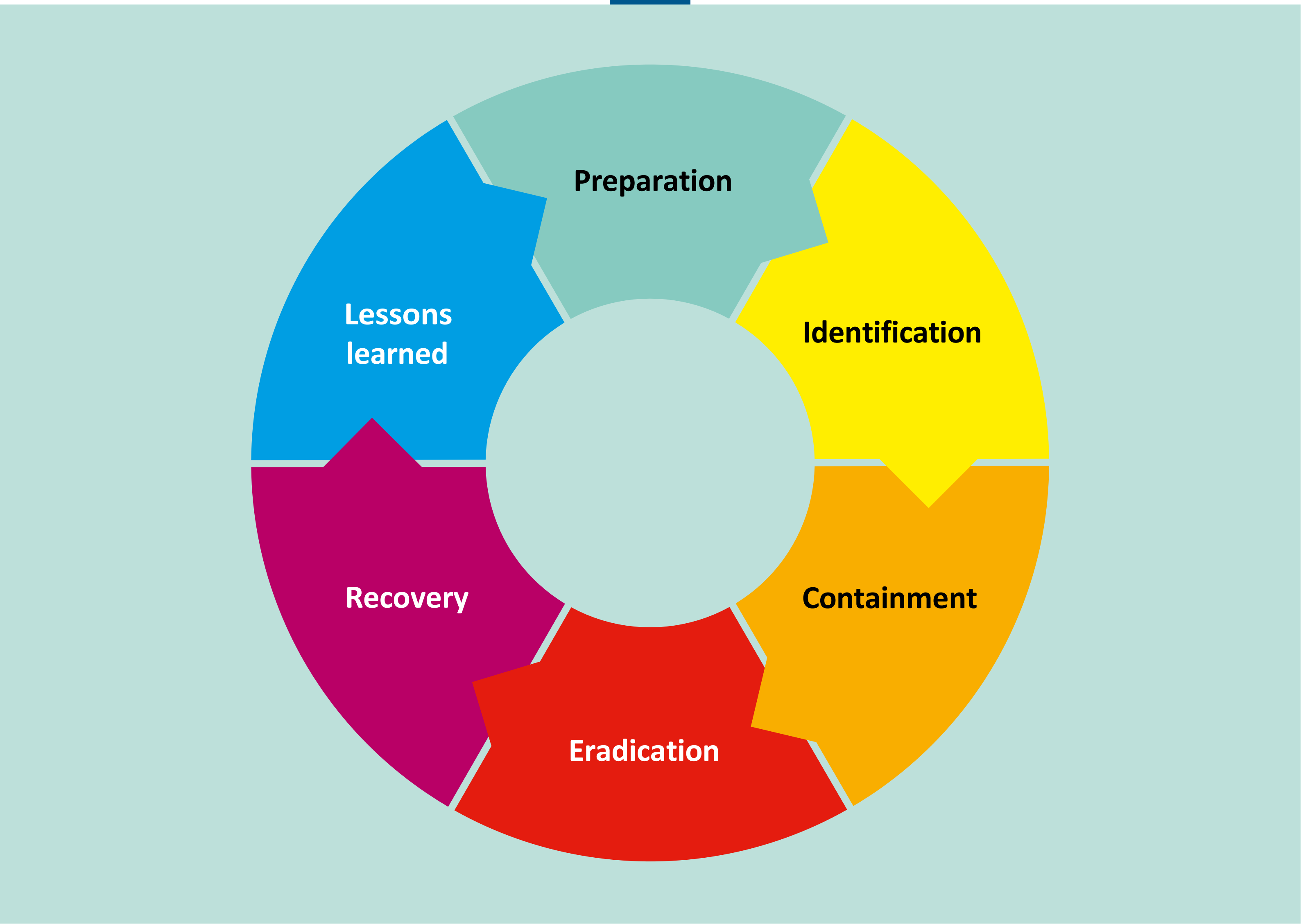
1. Restore impacted systems from a clean backup, taken prior to infection if these backups are available.
2. For systems not restorable from backup, rebuild the machines from a known good image or from bare metal.
3. Remediate any vulnerabilities and gaps identified during the investigation.

4. Reset passwords for all impacted accounts and/or create replacement accounts and leave the impacted accounts disabled permanently.
5. Continue to monitor for malicious activity related to this incident for an extended period.
    1. Alerts should be configured to aid in quick detection and response.

Lessons Learned

1. Conduct a meeting after the incident to discuss the following:
    1. What things went well during the investigation?
    2. What things did not go well during the investigation?
    3. What vulnerabilities or gaps in the organization's security status were identified?
        1. How will these be remediated?
    4. What further steps or actions would have been helpful in preventing the incident?
    5. Do modifications need to be made to any of the following:
        1. Network segmentation
        2. Firewall configuration
        3. Application security
        4. Operating System and/or Application patching procedures
        5. Employee, IT, or CSIRT training
2. Create and distribute an incident report to relevant parties.
    1. A primary, and more technical, report should be completed for the CSIRT.
    2. An executive summary should be completed and presented to the management team.

Malware Incident Response Plan04



1.1.1 Version managment

Version	Reason / amendments	Date
0.1	First draft	Nov. 2021
0.3	Review from NCSC theme incident response processes	Nov. 2021
0.8	Review within NCSC unit operation	Jan. 2022
0.9	External review	March 2022
1.0	Final format	May 2022
1.0	English translation	June 2022

This document was produced with contributions from Ahold Delhaize, the Betaalvereniging, CIBG, Equens and the Police.

1.1.2 Permitted distribution: TLP WHITE

(Traffic Light Protocol)

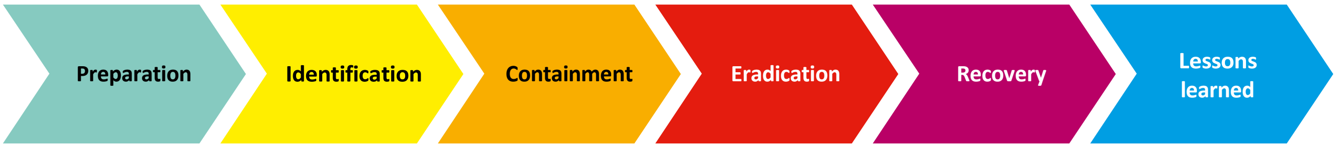
This guide contains the label TLP: WHITE and is distributed by the NCSC. The NCSC uses the Traffic Light

Protocol (TLP) to define
clearly and unambiguously what may be done with the information it provides. If information has a TLP designation, you will know with whom you may share it. This is described in the First standard (www.first.org/tlp). Recipients may share the information from this guide within their organisation and outside it, and the information may also be published.

We welcome your responses at info@ncsc.nl

Contents

Intended use of this plan



This plan is intended to prepare for and support incident response. Also known as a playbook, this plan serves organisations that have been, or think they may be, affected by a ransomware attack.
It is important to stress that good preparation is essential for an effective incident response. Ransomware can be a serious threat to (ICT) services for an organisation with a long-term and costly impact. In the light of such a potentially serious incident, it is good not to have to think about what to do from scratch, but to have an initial outline to work from.

This document is organised according to the steps described in the SANS incident response cycle[1]. If it is used to increase resilience to a ransomware incident, the first phase will be particularly important. It includes a wide range of aspects that will not suit all organisations equally. First of all, these are basic measures that can be used in recovery operations. In addition, there are more advanced measures to limit the impact of an attack or to detect an attack early. Due to the diverse nature of the measures, their implementation will also vary greatly. Existing measures can sometimes be tightened up to make them more effective. In other cases, the introduction involves an entire project, including appropriate processes and procedures.

When an organisation has already been affected by a ransomware attack, an effective response is essential and the phases from 'identification' onwards can provide a handle for the approach.

When using this plan, it is important to select only the relevant parts and translate them into the current situation. In addition, specific measures and activities for the organisation will have to be added in order to obtain an appropriate approach.

[1] The SANS Incident Handler's Handbook can be found at: https://www.sans.org/white-papers/33901/

Incident response

1.1.3 Definition response

For the purpose of this incident response plan, we define a **ransomware incident** as a digital attack that disables systems or files by encrypting them and holding data hostage. This hostage-taking is accompanied by extortion, whereby decryption is offered in return for a payment, usually in crypto-currency.

There are variations of ransomware extortion where, in addition to encryption, data is also stolen and threatened to be leaked if payment is not made (*double-extortion*) and where there are threats to disclose data to customers or to extort customers with the captured data (*triple-extortion*).

Appendix 1 contains a schematic representation of how a ransom- ware attack works, as described by the New Zealand National CERT (CERT NZ).

It is important to note that *ransomware is not just a technical problem.* In most cases, this involves serious, organised cybercrime. The police and the Public Prosecution Service are making efforts to combat this, but can only do so if cooperation is sought with them. This can be done by reporting the matter to the police.

When carrying out incident response, it is important to always keep a number of points of attention in mind. When resolving the disruption under pressure, these are easily lost out of sight. We list these below.

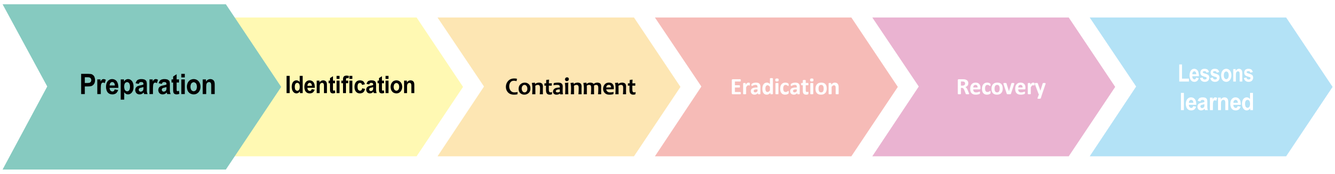
Points of attention for the incident

- Adhere to agreed incident response procedures and agreements;
- Proceed systematically;
- Make notes of your findings and activities (keep a log with date and time);
- When communicating and recording, confine yourself to facts, explicitly state what conclusions are drawn and avoid assumptions;
- Make sure that all those involved are kept informed of the current status and information;
- Communicate regularly and announce the next communication moment each time;
- Stay calm and keep in contact with the incident response team, CERT or CSIRT.

1.1.4 Communication

Communication is one of the strategic processes that help manage a disaster and/or crisis. For the internal organisation, it is important to offer employees clarity in order to prevent noise and unrest on the shop floor. To the outside world, communication is used to protect and/or restore the organisation's reputation and trust. This requires that as much uncertainty as possible be removed by carefully providing information, offering a perspective for action and making sense of what is happening. Stakeholders benefit most from open communication to limit consequential damage.

Preparation



In preparing for this type of incident, the following actions can be carried out per theme.

Continuity management

- Where appropriate, there will be a need for an integrated approach coordinated with network partners. Therefore, have contracts and service level agreements (SLAs) in place that regulate the presence and availability of the partners involved;
- Ensure that there are 24x7 standby managers on duty for the critical facilities. Pay attention to the application of and compliance with the terms and conditions of employment law;
- Have images (quickly) available to provide critical systems with a basic setup when deploying in a clean environment;
- Provide (rapidly) available spare hardware and available software to redeploy critical systems in a clean environment;
- Provide a recovery plan (dependencies, manner and order of recovery, responsibilities, system owners) of the ICT systems and the critical systems and test and update this regularly.

1.1.5 Back-up

- Determine what form of backup (incremental or full) is necessary and what retention time should be used;
- Provide a periodic offline backup of central and decentralised data;
- Ensure that all systems and virtual machines (VMs) are periodi- cally backed up;
- Check each backup result and periodically the backup process for possible errors;
- Regularly verify the integrity of the backup (by performing a restore, for example);
- Regularly test the backup against the agreed recovery point objective (RPO) and recovery time objective (RTO) (*see related information*);
- Store backups or backup media offline and off-site;
- Ensure that online and offline backups cannot be accessed using the same accounts; use accounts other than standard manage- ment accounts (including multi-factor authentication).

Design and design principles

- Segment the network according to both functionality and security level. Preferably follow the *zero trust* principle (*see related information*);
- Apply system hardening according to vendor guidelines or CIS benchmarks (*see related information*);
- Give users and administrators minimum rights, apply the principle of least privilege;
- Use a secure VPN solution that complies with TLS guidelines (*see related information*);
- Only connect management interfaces to a management (V)LAN;
- Use strong passwords and do not reuse them. Where possible, supplement authentication with multi-factor authentication (MFA) (*see related information*);
- Limit the use of local administrative accounts;
- Ensure that local administrative accounts on different systems have different (random) passwords. For example, use the Microsoft Local Administrator Password Solution (LAPS);
- Limit, protect and monitor the use of Active Directory domain administrator accounts;
- Turn off access to systems via RDP unless there is no other way. If no alternative is available, secure remote access channels and RDP with, for example, MFA and a VPN solution, and log their use.

Inventory and configuration management

- Identify critical systems and determine the impact when they are affected by ransomware;
- Provide an up-to-date and complete overview of systems and interdependencies;
- Record the configuration of systems with each change;
- Develop and maintain infrastructure designs containing critical systems and data flows. Take account of supply chain partners and outsourced services;
- Ensure that product maps and architectural records of the critical facilities are available and up-to-date.

Monitoring and detection

- Ensure the security of the email environment, including scanning for attachments or internet links;
- Provide (secure and centralised) logging in the network of:
- Executed (powershell) scripts and attempted excution of (powershell) scripts;
- Event-Ids for authentication;
- Event-Ids for creating services and persistent processes;
- (Large) outgoing data streams;
- Event-Ids for creation or modification of (privileged) accounts
- Use canary files (documents or files that should not be used and modified) to detect unauthorised changes to the file system;
- Monitor the use of sensitive management accounts, such as Domain Admin accounts.

Processes and procedures

1.1.6 Communication

- Take account of the breakdown of regular communication channels (telephone, email, address book access, chat), prepare, test and keep up-to-date confidential alternatives or fall-back options;
- Define an internal and external communication strategy. Ensure that stakeholders (employees, spokespersons/press officers, chain partners, customers, board of directors, data protection officers, etc.) are informed in a timely manner and take into account:
  - The purchasing department may be able to help by providing an overview of suppliers;
  - Involve the legal department in the preparation and possibly have an external communication manual approved in advance;
- Determine the communication strategy when stolen data is published, including:
  - Which senders and recipients are important;
  - Which messages should be sent;
  - Which supervisory authority or authorities (including the Dutch Data Protection Authority) must be informed;
  - Which other organisations need to be informed (NCSC, police, etc.);
- Determine a strategy for dealing with the ransom note. Contacting the hostage takers can be important in order to determine whether data has been stolen and what data sources have been accessed. In addition, criminals should share infor- mation during negotiations; this increases the chances of successful detection. *It is important to note that having contact with the hostage takers does not mean that a ransom has to be paid.* The urgent advice from the police and from the Government remains not to pay a ransom after a ransomware attack, as this maintains the criminal revenue model.[2]

[2] https://www.nomoreransom.org/en/ransomware-qa.html
https://www.politie.nl/nieuws/2020/februari/6/00-politie-%E2%80%98niet-betalen-bij-ransomware.%E2%80%99.html
https://www.tweedekamer.nl/kamerstukken/kamervragen/detail?id=2021Z16018&did=2021D37453

Moreover, payment does not guarantee that the problem is resolved: there are known cases where the decryption does not take place (completely) even after payment; the attacker may still be in your network even after payment; the attacker may have stolen your data and blackmail you again later (the perpetrator now knows that you are willing to pay). For the contact about the ransom note, take account of:

- Who should be called in to hold a discussion with the hostage takers;
- What information must be established in a negotiation/ discussion;
- How a ransom demand is handled;
- Who reports the matter to the police and when is it reported.

1.1.7 Incident response

- Prepare an incident response plan, including:
  - Who should be involved in a cyber security incident;
  - How, on the basis of which criteria and by whom is it determined that there is a security incident;
  - Who is responsible for resolving the incident;
  - How and when to connect to regular (ITIL) incident management procedures;
- Know who the internal key players and external stakeholders are;
- Make the mandate of those involved explicit, especially which officer has the power to switch off a service or facility;
- Describe the role and structured work process of the incident response team. Also describe the desired requirements and competences per role of the team, in the form of job descriptions;
- Introduce a standard structure for crisis consultations, in which situational awareness can be shared and decisions can be reached. A process of crisis decision making within a crisis management team could be:
  1) establish the situation (perception of data);
  2) comprehension (determine the meaning of the situation, identify the issues and analyse them and set the direction);
  3) take action (determine what to do with the issues; can we solve them ourselves, who do we need to involve and what strategic decisions do we need).
  And practice the consultation according to this structure;
- Ensure that the members of the incident response team have sufficient rest and sleep during the performance of the incident response;
- Equip those involved with the means to communicate quickly and easily as a team even outside office hours. Make it possible for those involved to work from the office environment (including the back-up location) outside office hours;
- As various ransomware incidents have shown that ransomware is often executed on the systems on Friday evenings, it is useful to take this into account for picket roles and the availability of incident response team members;Arrange for a contract with a service provider or incident response party to support and carry out, for example, recovery and forensic investigations;

- Simulate and practice a ransomware attack with employees. Evaluate this exercise and use it as input to update the incident response plan where necessary;
- Take into account guidelines, legislation and regulations (e.g. for informing supervisors, stakeholders and authorities) and incorporate this in the incident response plan. Also take into account the possibility of making a voluntary WBni report or a mandatory WBni report to the NCSC or the CSIRT DSP;
- Be prepared to report the matter to the police. This will give the police better insight into the phenomenon of ransomware and enable them to give it the appropriate priority. Refer to the brochure 'Samen tegen Cybercrime, Stappenplan voor IT-specialisten' (Together against Cybercrime, Step-by-step plan for IT specialists), which has been drawn up by the police to take measures that support the investigation of crime (*see related information*). Making a report or announcement can also prevent new attacks. This allows the police to warn other organisations or disable servers with malicious software.

Accounts and rights

- Delete unnecessary or unused user accounts and groups;
- Assign minimum domain, admin and root privileges to accounts;
- Restrict access to domain controllers to a separate domain administrator group;
- Limit the rights of the domain administrator group and use the member accounts only for administration on the domain controllers. Create separate administrator accounts for other management tasks;
- Log the use and login of management accounts (both successful and unsuccessful login attempts).

1.1.8 Miscellaneous

- Make sure that the network can be monitored on:
  - Which (unknown) files have been or are being executed;
  - Which (powershell) scripts have been or are being executed;
  - Which 'lateral movement' between workstations/endpoints is taking place or has taken place;
  - Which (large amounts of) data is or has been exfiltrated;
  - Who logged on to which system or used resources;
- Establish a procedure for forensic image creation of workstations and servers and test it regularly;
- Have an implemented patch and upgrade policy and update systems (servers and workstations) regularly; base the priority and schedule of patching on the severity of the remedied vulnerabilities;
- Provide an emergency patch and update process to immediately mitigate critical vulnerabilities.

Technical measures

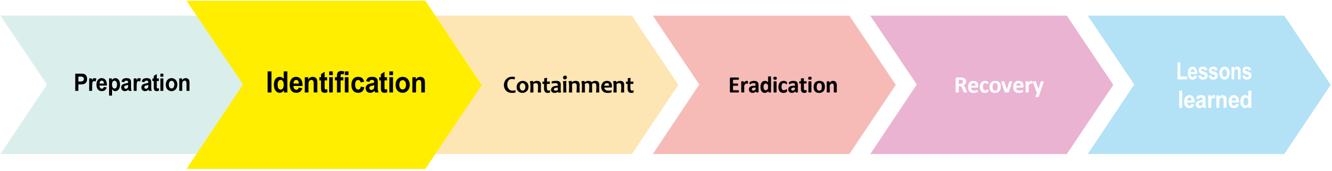
- Install an Endpoint Detection and Response (EDR) tool on both clients and servers;
- Implement network segmentation based on function (development, test, acceptance and production) and data classification (public, internal, confidential, secret, personal data, special data);
- Implement multi-factor authentication (MFA);
- Maintain and check antivirus software; scan any software downloaded from the internet before running it;
- Centrally disable macros in office software so that macros in infected files cannot be executed;
- Turn off following web links or opening images in emails;
- Turn off the Remote Desktop Protocol (RDP) on the internet side (ransomware often spreads by malicious actors who have compromised organisations via RDP);
- Check the periphery of the network for the presence of management interfaces on the outside and switch them off;
- Consider using PowerShell constrained language mode to limit PowerShell usage;
- Consider applying additional PowerShell logging measures, such as: Module logging, Script-Block logging and Transcript logging;
- If you use Windows operating systems, consider applying Applocker and Windows Defender Application Control to limit the use of unwanted scripts and software;
- Use the 'Protected Users' Active Directory group in Windows Active Directory for privileged user accounts to make pass-the-hash attacks more difficult;
- Consider application whitelisting;
- Do not install additional software on domain controllers or on other systems, and remove already installed software that is not needed;
- Disable unnecessary services on domain controllers and other servers, and disable the print spooler service on domain controllers;
- Block internet connectivity on the domain controllers. Updates can be retrieved via a WSUS solution;
- Consider implementing additional Local Security Authority (LSA) security on Windows servers (the LSA process validates (local and remote) user login and ensures the application of security policies);
- Determine and configure the use of Bit-Locker or other disk encryption (if not used, it can be used by attackers);
- Block the use of unauthorised USB devices and configure the permitted use of authorised USB devices;
- Consider filtering outgoing traffic on the firewall, configure which applications and servers are allowed to communicate with the outside world.

Employee awareness

- Employees include temporary staff, advisors and seconded staff.
- Ensure there is knowledge and awareness among employees about:
  - Phishing variants and how to recognise them;
  - Identifying social engineering;
  - The spread of malware and ransomware;

  - Recognising a ransomware infection and how to respond to this;
  - How to report suspicious observations or possible contaminations;
  - Using different passwords for different systems and environments (support employees in this by offering a password manager);
  - The desired use of company property and mobile devices;
  - The organisation's social media policy;
- Make it easy for employees to report suspicious email messages, for example by providing a menu option or button for this;
- Make a list of key officials and make them aware of the possible espionage risks due to their function or position within the organisation;
- Provide a policy plan for education, training and exercise of, among others, the above aspects, and implement the plan

Identification


Preparation
Identification
Containment
Eradication
Recovery
Lessons learned

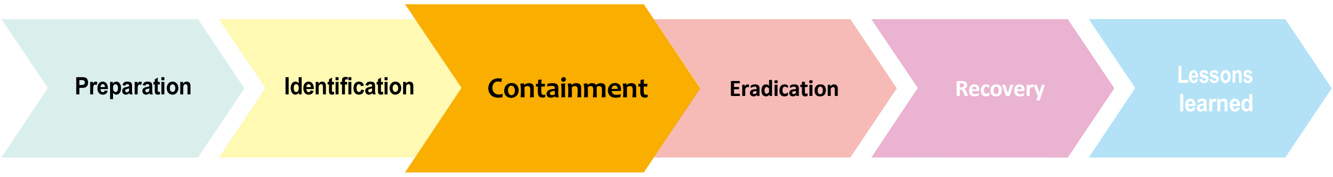
Preliminary remark: A ransomware incident may manifest itself with a large-scale disruption of (ICT) services because file systems have been encrypted. This may require an immediate start to restoring a (clean) environment in order to resume services as soon as possible. *However, it is still necessary to run through the incident response cycle in parallel with recovery, starting with identification.* After all, it is important to deny malicious actors access to the network and keep them from regaining access to the network in the future.

The following may be an indication of a ransomware incident. This also includes a number of activities, which can be carried out for identification purposes:

- Unusual invoices or other business emails, possibly with malicious attachments or links;
- Ransomware messages on the file system;
- Ransomware messages on the screen;
- Ransomware messages via email;
- Employees report that they can no longer open their files;
- Large numbers of files are (successively) modified on a (network) file system;
- An unusual (large) amount of data is diverted;
- System analysis leads to identification of server-side encryption. Investigate:
  - In Windows under computer management under 'Sessions' and under 'Open Files'; check for connected systems/users;
  - Ownership of encrypted files; check the account that is writing these files;
  - The RDP event log; check for unexpected successful RDP connections;
  - The Windows Security log and SMB log; check for authentication events;
  - Network communication via the SMB protocol to identify open connected systems;
- Unusual activity is observed on a system or malware is found that can encrypt a file system (or can download modules that can encrypt a file system). Examination:
  - Unusual binaries;
  - Forensic images of memory;
  - Unusual processes;

  - Unusual tasks in the Task Scheduler
  - Unusual patterns of email attachments;
  - Unusual network or web browsing activity, for example TOR traffic or traffic to cryptocurrency payment sites;
- Malicious communications or network traffic may be taking place. These include:
  - Known patterns of exploit kits;
  - Connections to (known) C2 servers;
  - Unusual network traffic or web browsing activity, for example TOR traffic or traffic to cryptocurrency payment sites;
  - Emails with links to suspicious or malicious websites;
  - Unusual attachments in emails (attachments of a type that an employee does not normally receive, attachments from a sender who does not normally send attachments or attach- ments from an unknown sender);
- Announcements are made of a successful ransomware attack by known actors on the dark web;
- Exfiltrated data or files from a ransomware attack are offered on the dark web;
- A phishing attack is carried out with characteristics that can be traced back to known ransomware attacks (use DMARK logs or DNS logs if necessary);
- After observing a ransomware attack, provide an up-to-date situational picture (which systems have been affected and what is the function of those systems, who is responsible for that system) and an impact assessment so that measures to be taken are consistent with this;
- It is important to identify 'Patient Zero' in order to understand how the attacker got in and to deny access at a later stage (e.g. look for where unusual activity occurred after receiving a phishing email, from where C2 communication occurs or where common ransomware-related tooling is used, such as installation of a keylogger, exploitation of a vulnerability using Metasploit, execution of Mimikatz or Cobalt Strike);
- Based on the current situational picture, determine whether it is necessary to make a voluntary or mandatory Wbni report to the NCSC or to CSIRT DSP;
- Monitor supply chain partners (customers, suppliers or coopera- tion partners) for reports of possible ransomware infections.

Containment

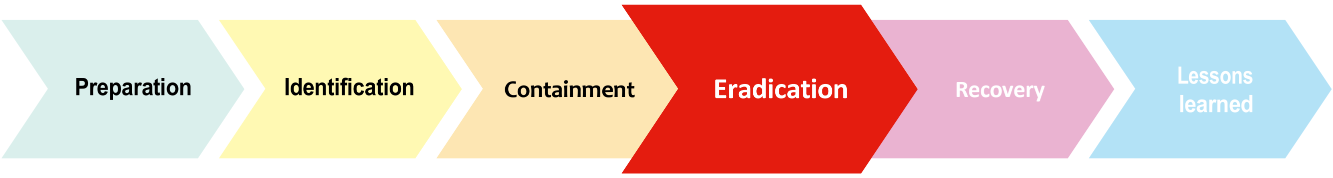


To contain the consequences of this type of incident, the following actions can be taken:

- Immediately disconnect systems from the network (on all interfaces: wired, Wi-Fi or mobile) that have been identified or are suspected of being compromised (with ransomware) (disconnection is also possible by activating aeroplane mode);
- Do not turn systems off, but put them in sleep mode or possibly hibernate mode (if available, e.g. on laptops). This is so as not to disrupt the system's condition and thus obtain the best possible image, to prevent the loss of any key material present and not to lose any forensic traces for possible investigation;
- In the event of a major attack, consider disconnecting network infrastructure, such as Wi-Fi, routers and switches and internet connectivity; if possible, disconnect networks or network parts not yet affected by the ransomware;
- Immediately disconnect external devices, such as USB/external drives, mobile phones or other devices that may become infected;
- Disconnect the network file storage if a system cannot be isolated or disconnected from the network;
- Block or deactivate all accounts (potentially) involved in the ransomware attack;
- Reset passwords and other forms of authentication for admini- strator and other system or service accounts (note: resetting the password of the KRBTGT service account must be performed twice in succession otherwise access with the old password will remain possible) (see related information);
- Reset user passwords;
- Remove write permissions on file systems from processes or accounts with which ransomware is executed;
- Check that MFA is still set on the accounts and for access to services where it is intended and correct where necessary if a malicious user has disabled MFA;
- Block traffic with potentially identified C2 servers;
- Submit the (characteristics of) as yet unknown malware found in the incident response process or forensic analysis to the endpoint security provider and the NCSC;
- Submit as yet unknown malicious URLs, domain names or IP addresses to the network security provider and the NCSC;
- Report the incident as soon as possible to prevent further damage (contact information can be found at the end of this document);

- Collect possibly relevant log files, such as: Windows Security logs, Email logs, Firewall logs and Linux System logs;
- If a supply chain partner is potentially infected, block the exchange of email and network traffic with this organisation until it is clear that the risk of infection has been eliminated;
- Consider informing the police in this incident response phase. There have been occasions when the police have been able to intervene in the channelling of information to leak pages. It may also be possible for the police to warn other (potential) victims in time. It is also relevant at this stage to think about securing evidence, such as communication channels and BTC addresses. Refer to the brochure 'Samen tegen Cybercrime, Stappenplan voor IT-specialisten' (Together against Cybercrime, Step-by-step plan for IT specialists), which has been drawn up by the police to support the investigation of crime (*see related information*).

Eradication



Preparation

Identification

Containment

Eradication

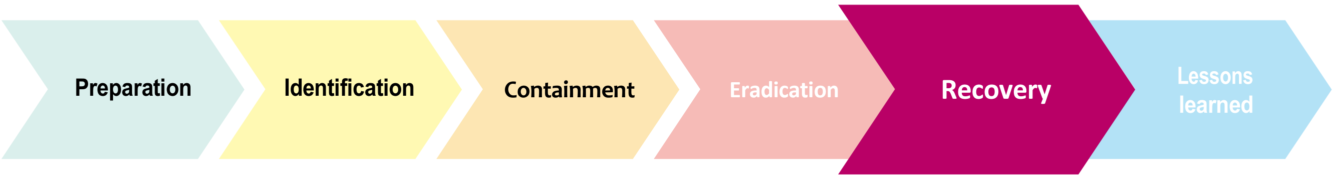
Recovery

Lessons learned

Note: *Do not proceed with eradication until it is clear that the entire* scope of the attack has been mapped and no new infected machines are found. Moving too quickly with eradication may inform an attacker of the incident response actions taken and may leave behind an attacker's backdoor or dormant malware.

- To eradicate the breach or impact of this type of incident, the following actions can be taken:
- Delete the malicious binaries and, if applicable, corresponding registry values from (centrally stored) compromised user profiles and systems (also consider %ALLUSERPROFILE%, %APPDATA% and %SystemDrive%). If cleaning is not possible, consider deleting (centrally) stored user profiles;
- Reinstall affected systems with a clean image after any locally stored data and files have been quarantined;
- Record metadata such as signatures and origin of the malware, domains and IP addresses and block known malware (communication);
- Update antivirus signatures so that the identified malware is blocked;
- Identify the system where the first breach occurred and remedy the cause or potential vulnerabilities.
- Implement the established internal and external communication strategy. Ensure that stakeholders (employees, chain partners, customers, board of directors, etc.) are informed in a timely manner.

Recovery

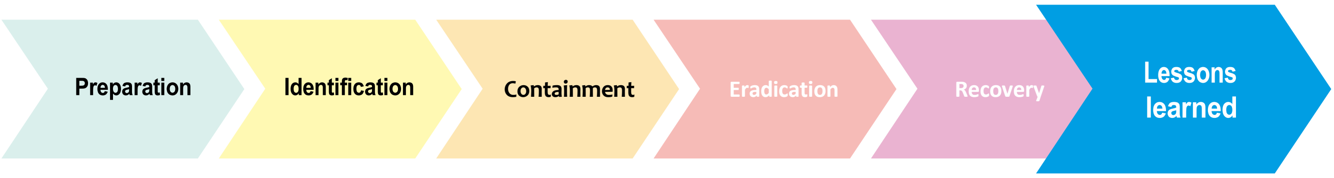


To recover from this type of incident, the following actions can be taken:

- In the event of a major attack, consider building the network and associated systems in parallel to the existing environment.
  Do not import systems or data without thoroughly checking them for the presence of malware. Do not connect systems to the clean environment that have been connected to the infected environment;
- If it is not possible to build a new environment parallel to the existing one in the event of a major attack with possible com- promise of the Active Directory, consider building a new permission structure with new accounts, including management and service accounts, and (permanently) deleting all old accounts;
- Only use carefully certified secure systems for recovery;
- Make sure all malicious binaries that were present are removed from the systems if they need to be reconnected and cannot be reconfigured;
- Check with the No More Ransom project (*see related information*) if there are any known decryption keys or software available for the ransomware used in this incident;
- Contact law enforcement agencies to report the incident and obtain possible decryption keys;
- Share (technical) information about the incident with the police. This can be by means of an official report, but also by providing information. This can assist with the (international) detection and disruption of offender groups and it can lead to the notifi- cation of other (potential) victims;
- Scan backups for malware before restoring. The malicious actors may have been in the network for a long time, so that malicious files could have ended up in the backups;
- Scan quarantined data and files and remove any malware found;
- Restore encrypted or compromised servers or systems from an uncompromised backup;
- Recover encrypted files from an uncompromised backup;
- If decryption or recovery from a backup fails and there is a data loss, a copy of the encrypted information can be retained. If a method of decrypting the information is found later, it can still be retrieved.

- Correct any unwanted configuration changes that may have been made by the malicious parties;
- Test and verify whether the abnormal behaviour (e.g. network traffic) has disappeared after restoring all systems and processes;
- Monitor the network intensively for some time to make sure that the attacker has disappeared from the network and cannot get back in;
- Upgrade and update outdated software and systems.

Lessons learned



Lessons can be learned from such incidents after recovery, which in turn can lead to further preparatory actions. As these lessons learned are specific to each incident, they cannot be determined in advance. However, it is vitally important to go through this phase. All preparatory actions already carried out can also be evaluated in this step. In order to obtain useful feedback for the lessons learned, an after-action review can be performed with those involved at the conclusion of the active incident response, so that experiences can be shared fresh from the experience.

The quality of reporting is improved if there is always someone present who performs the role of reporting at all stages so that all steps, decisions, documents, etc. are recorded correctly, on time, completely and in a verifiable manner (in addition to the individual logs kept by employees).

It is recommended that the lessons learned be included in a report. It is recommended to pay attention to the following issues, among others:

- Dissemination: who will receive the report;
- Target group of the report;
- Initial infection;
- Activities and timeline;
- Targeted systems;
- Impact on availability;
- Influence on or dependency on (supply chain) partners, custo- mers, suppliers or other stakeholders;
- Characteristics of the ransomware used (IOCs);
- Risks of possible leaked data in the outside world;
- Effectiveness and execution of the incident response process (what went well and what could be improved);
- Costs and lead time of the incident;
- Which documentation needs to be modified on the basis of the lessons learned and who will do this;

- How do you inform the organisation of these changes;
- Changes to be implemented to prevent future similar incidents or to reduce their impact, relating to:
  - System adaptation and technical modifications;
  - Adjustments to procedures and policies;
  - Adjustments to incident response procedures or to specific incident response plans;
- Share found indicators and report with the NCSC so that other organisations can be alerted or informed.

Relatedinformation

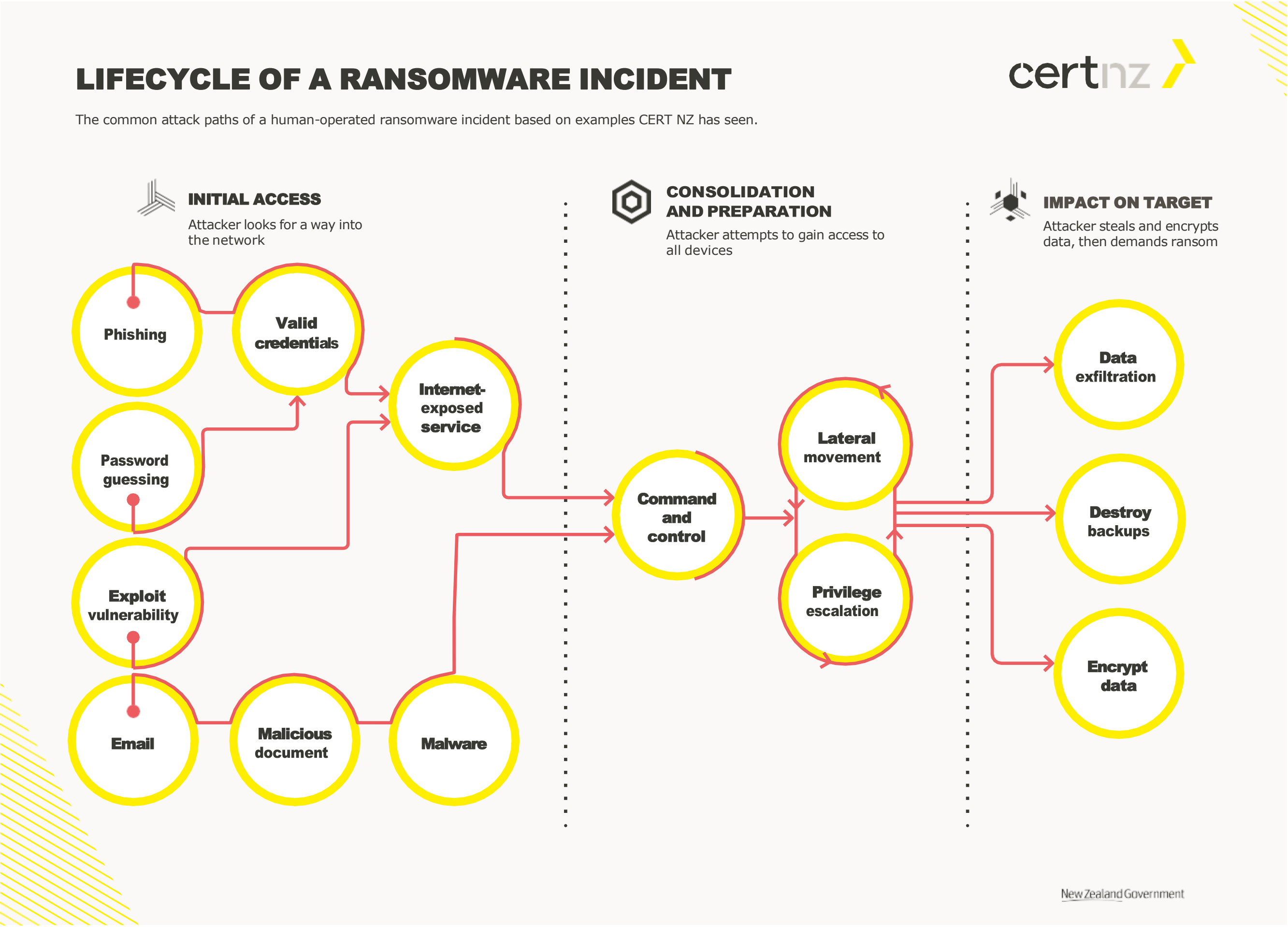
Sources of information

Document	*Location*
NCSC factsheet ransomware	https://english.ncsc.nl/publications/factsheets/2020/june/30/factsheet-ransomware
NCSC factsheet 'Prepare for Zero Trust'	https://english.ncsc.nl/publications/factsheets/2021/augustus/18/factsheet-prepare-for-zero-trust
NCSC ICT security guidelines for Transport Layer Security (TLS) v2.0	https://english.ncsc.nl/publications/publications/2019/juni/01/it-security-guidelines-for-transport-layer-security-tls
NCSC factsheet mature authentication – use of secure authentication tools	https://english.ncsc.nl/publications/factsheets/2022/juni/9/factsheet-mature-authentication---use-of-secure-authentication-tools
No More Ransom project	https://www.nomoreransom.org/en/index.html
Ransomware Guide (CISA)	https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C_.pdf
Ransomware Infographic (Police)	https://www.politie.nl/binaries/content/assets/politie/onderwerpen/ransomware/infographic-cybercrimes-ransomware.pdf
Back-up strategy	https://business.gov.nl/running-your-business/business-management/cyber-security/all-about-good-backups/ https://www.digitaltrustcenter.nl/back-up/geavanceerde-informatie-over-back-ups
CIS benchmarks	https://www.cisecurity.org/cis-benchmarks/
Microsoft white paper 'Mitigating Pass-the-Hash and Other Credential Theft, version 2'	http://download.microsoft.com/download/7/7/A/77ABC5BD-8320-41AF-863C-6ECFB10CB4B9/Mitigating-Pass-the-Hash-Attacks-and-Other-Credential-Theft-Version-2.pdf
Samen tegen Cybercrime, Stappenplan voor It-specialisten (Together against Cybercrime, Step-by-step plan for IT specialists)	https://www.politie.nl/binaries/content/assets/politie/algemeen/algemeen/brochure-stappen-plan-cybercrime.pdf

Contact details

Organisation	*Contact details*
NCSC CERT service	cert@ncsc.nl
NCSC general	info@ncsc.nl
Police (report)	https://www.politie.nl/aangifte-of-melding-doen

Appendix1:Schematic representation of a ransomware attack


LIFECYCLE OF A RANSOMWARE INCIDENT
The common attack paths of a human-operated ransomware incident based on examples CERT NZ has seen.
certnz
INITIAL ACCESS
Attacker looks for a way into the network
CONSOLIDATION AND PREPARATION
Attacker attempts to gain access to all devices
IMPACT ON TARGET
Attacker steals and encrypts data, then demands ransom
Phishing
Valid credentials
Password guessing
Internet-exposed service
Exploit vulnerability
Email
Malicious document
Malware
Command and control
Lateral movement
Privilege escalation
Data exfiltration
Destroy backups
Encrypt data
New Zealand Government

Source: https://www.cert.govt.nz/it-specialists/guides/how-ransomware-happens-and-how-to-stop-it/

Malware Incident Response Plan 05:

INCIDENT RESPONSE METHODOLOGY

IRM #7 WINDOWS MALWARE DETECTION

Live Analysis on a suspicious computer

IRM Author: CERT SG
Contributor: CERT aDvens
IRM version: 2.0
E-Mail: cert.sg@socgen.com
Web: https://cert.societegenerale.com
Twitter: @CertSG

SOCIETE
GENERALE

ABSTRACT

This Incident Response Methodology is a cheat sheet dedicated to handlers investigating on a precise security issue.

WHO SHOULD USE IRM SHEETS?

- Administrators
- Security Operation Center
- CISOs and deputies
- CERTs (Computer Emergency Response Team)

.1.9 Remember: If you face an incident, follow IRM, take notes. Keep calm and contact your business line's Incident Response team or CERT immediately if needed.

→ IRM CERT SG: https://github.com/certsocietegenerale/IRM

→ IRM CERT aDvens (French version): https://github.com/cert-advens/IRM

INCIDENT HANDLING STEPS

6 STEPS ARE DEFINED TO HANDLE SECURITY INCIDENTS

1. Preparation: get ready to handle the incident
2. Identification: detect the incident
3. Containment: limit the impact of the incident
4. Remediation: remove the threat
5. Recovery: recover to a normal stage
6. Lessons learned: draw up and improve the process

IRM provides detailed information for each step of the incident response process. The steps come from NIST Computer Security Incident Handling Guide.

PREPARATION

OBJECTIVE: ESTABLISH CONTACTS, DEFINE PROCEDURES, GATHER INFORMATION TO SAVE TIME DURING AN INCIDENT.

- Deploy an EDR solution on endpoints and servers
  - This tool became one of the cornerstones of incident response in case of ransomware or in large scale compromise, facilitating identification, containment, and remediation phases.
  - Launch EDR Search and AV scan with IOC explicit rules and get first indicators for remediation progress following.
  - Set your EDR policies in prevent mode to prevent unnecessary business disruption.
- In absence of EDR, a physical access to the suspicious system should be given to the forensic investigator. Physical access is preferred to remote access, as the hacker could detect the investigations done on the system (by using a network sniffer for example).
- A physical copy of the hard-disk might be necessary for forensic and evidence purposes. Finally, if needed, a physical access could be needed to disconnect the suspected machine from any network.
- Acquisition profiles for EDR or tools like FastIR, DFIR Orc, KAPE, DumpIt, FTK Imager, WinPmem must be prepared and tested.
- A good knowledge of the usual network activity of the machine/server is needed. You should have a

  file on a secure place describing the usual port activity, to compare efficiently to the current state.
- A good knowledge of the usual services running on the machine can be very helpful. Don’t hesitate to ask a Windows Expert for his assistance, when applicable. A good idea is also to have a map of all services/running process of the machine.

Endpoints

- Ensure that the monitoring tools are up to date.
- Deploy Sysmon, SmartScreen and apply recommendation baselines from ANSSI and CIS.
- Establish contacts with your network and security operation teams.
- Make sure that an alert notification process is defined and well-known from everyone.
- Make sure all equipment are synchronized with the same NTP.
- Select what kind of files can be lost / stolen and restrict the access for confidential files.
- Make sure that analysis tools are up, functional (Antivirus, EDR, IDS, logs analyzers), not compromised, and up to date.
- Install from the same original master.

IDENTIFICATION

OBJECTIVE: DETECT THE INCIDENT, DETERMINE ITS SCOPE, AND INVOLVE THE APPROPRIATE PARTIES.

The family of malware identified will impact the next steps of the incident response. Investigation will be faster for a Potentially Unwanted Software or a Miner. Stealer, Dropper or Ransomware family will imply a deeper analysis and may lead to another kind of incident (please refer to Large scale malware compromise, Ransomware, Windows Intrusion Detection or Worm Infection if needed).

General signs of malware presence on the desktop

Several leads might hint that the system could be compromised by malware:

- EDR, HIDS, Antivirus software raising an alert, unable to update its signatures, shutting down or unable to run manual scans.
- Unusual hard-disk activity: the hard drive makes huge operations at unexpected times.
- Unusually slow computer: sudden, unexplained slowdowns not related to system usage.
- Unusual network activity: Slow internet connection / poor network share performance at irregular intervals.
- The computer reboots without reason.
- Applications crashing unexpectedly.
- Pop-up windows appearing while browsing the web. (sometimes even without browsing).
- Your IP address (if static) is present on one or more Internet Blocklists.
- People are complaining about you e-mailing them/reaching them by IM etc. while you did not.

If the issue is considered as strategic (sensitive resources access), a specific crisis management cell should be activated. i.e. Large Scale Compromise IRM-18

Most of the above guidance is inspired by SANS Institute posters: https://www.sans.org/posters
It's always better to run several of these tools than only one.

IDENTIFICATION

1 – Evidence acquisition

WARNING (VOLATILE

DATA):

BEFORE CARRYING OUT ANY OTHER ACTIONS, MAKE SURE TO MAKE A VOLATILE MEMORY CAPTURE
BY DOWNLOADING AND RUNNING FTK IMAGER, WINPMEM OR ANOTHER UTILITY FROM AN EXTERNAL DRIVE.
VOLATILE DATA PROVIDES VALUABLE FORENSIC INFORMATION AND IS STRAIGHTFORWARD TO ACQUIRE.

- Volatile data:

Volatile data is useful to perform analysis on command line history, network connections, etc. Use "Volatility" if possible.

- Take a triage image:

Use tools like EDR, FastIR, DFIR Orc, KAPE with preconfigured profiles.

Or

- Full disk copy image:

With tools like dd, FTKImager, etc.

Warning: you may need admin privileges on the machine or a write-blocker (physical or logical) depending on the use case.

2 – Memory analysis:

- Look for rogue processes
- Review process DLLs and handles
- Check network artifacts
- Look for code injection
- Check the presence of rootkits
- Dump suspicious processes for further analysis

If the issue is considered as strategic (sensitive resources access), a specific crisis management cell should be activated. i.e. Large Scale Compromise IRM-18

Most of the above guidance is inspired by SANS Institute posters: https://www.sans.org/posters
It's always better to run several of these tools than only one.

IDENTIFICATION

3 – Identify persistence mechanisms:

Persistence can be allowed through different techniques including:

- Scheduled tasks
- Service replacement
- Service creation
- Auto-start registry keys and startup folder
- Dll search order hijacking
- Trojaned legitimate system libraries
- Local Group Policy
- MS office add-in
- Pre-boot persistence (BIOS/UEFI/MBR alteration)

You may consider using Microsoft autoruns for a quick win.

4 – Check Event Logs

- Scheduled tasks log (creation and execution)
- Account Logon Events (check for out-of-office connections)
- Suspicious local account
- Malicious Services
- Clearing Event Logs
- RDP/TSE Logs
- Powershell Logs
- SMB Logs

5 – Super-Timeline

- Process evidence and generate a super-timeline with tools like Log2timeline.
- Analyze the generated timeline with TimelineExplorer or glogg for example.

6 – To go further

- Hash lookups
- MFT anomalies and timestamping
- Anti-virus/Yara analysis/Sigma :

Most of the above guidance is inspired by SANS Institute posters: https://www.sans.org/posters
It's always better to run several of these tools than only one.

IDENTIFICATION

- Mount the evidence in a read-only mode. Run Anti-virus scan or multiple Yara files for a quick- win detection.
- Please note that unknown malware may be not detected.

If the issue is considered as strategic (sensitive resources access), a specific crisis management cell should be activated. i.e. Large Scale Compromise IRM

Most of the above guidance is inspired by SANS Institute posters: https://www.sans.org/posters
It's always better to run several of these tools than only one.

CONTAINMENT

OBJECTIVE: MITIGATE THE ATTACK'S EFFECTS ON THE TARGETED ENVIRONMENT.

WARNING (VOLATILE DATA):

MEMORY AND SELECTIVE VOLATILE ARTIFACTS' ACQUISITION MUST BE CARRIED OUT BEFORE THE FOLLOWING STEPS HAVE TAKEN PLACE.

If the machine is considered critical for your company's business activity and can't be disconnected, backup all important data in case the hacker notices you're investigating and starts deleting files.

- If possible, isolate the machine via EDR.

OR

- If the machine is not considered critical for your company and can be disconnected, shut the machine down the hard way, removing its power plug. If it is a laptop with a battery on, just push the "off" button for a few seconds until the computer switches off.

Send the suspect binaries to your CERT, or request CERT's help if you are unsure about the malware's nature. The CERT should be able to isolate the malicious content and can send it to all AV companies, including your corporate contractors. (The best way is to create a zipped, password-encrypted file of the suspicious binary.)

Offline investigations should be started right away if the live analysis didn't give any result, but the **system should still be considered compromised.**

- Inspect network shares or any publicly accessible folders shared with other users to see if the malware has spread through it.
- More generally, try to find how the attacker got into the system. All leads should be considered. If no computer proof of the intrusion is found, never forget it could come from a physical access or a complicity/stealing of information from an employee.
- Apply fixes when applicable (operating system and applications) in case the attacker used a known vulnerability.

REMEDIATION

OBJECTIVE: TAKE ACTIONS TO REMOVE THE THREAT AND AVOID FUTURE INCIDENTS.

WARNING: ONLY START REMEDIATING ONCE YOU ARE 100% SURE THAT YOU HAVE WELL SCOPED UP AND CONTAINED THE PERIMETER - AS TO PREVENT THE ATTACKER FROM LAUNCHING RETALIATION ACTIONS.

The most straight-forward way to get rid of the malware is to remaster the machine.

- Remove the binaries and the related registry entries.
- Find the best practices to remove the malware. They can usually be found on Antivirus companies' websites.
- Remove all malicious files installed and persistence mechanisms put in place by the attacker.
- Apply the EDR prevention mode for all identified IOCs.

RECOVERY

OBJECTIVE: RESTORE THE SYSTEM TO NORMAL OPERATIONS.

If possible, reinstall the OS and applications and restore user's data from clean, trusted backups. If deemed necessary, you may ask your local IT helpdesk to reimage the disk.

In case the computer has not been reinstalled completely:

- Restore files which could have been corrupted by the malware, especially system files.
- Change all the system's accounts passwords and make your users do so in a secure way.

- Reboot the machine after all the suspicious files have been removed and confirm that the workstation is not exhibiting any unusual behavior. A full, up-to-date AV and EDR scan of the hard-drive and memory are recommended.

If a user is at the origin of the compromise, you should reinforce security awareness campaigns.

For more details on authentication and infrastructure recovery, check the Large-scale malware compromise IRM-18

LESSONS LEARNED

OBJECTIVE: DOCUMENT THE INCIDENT'S DETAILS, DISCUSS LESSONS LEARNED, AND ADJUST PLANS AND DEFENSES.

Report

An incident report should be written and made available to all of the stakeholders.

The following themes should be described:

- Initial detection
- Actions and timelines
- What went right
- What went wrong
- Incident cost
- Indicators of compromise

Capitalize

Actions to improve malware detection and eradication processes should be defined to capitalize on this experience.
Profiles of acquisition tools can be tweaked to better match artifacts detected during the investigation.

INCIDENT RESPONSE METHODOLOGY

IRM #9 MALWARE ON SMARTPHONE

How to handle a suspicious smartphone

IRM Author: CERT SG **Contributor:** CERT aDvens **IRM version: 2.0**

E-Mail: cert.sg@socgen.com
Web: https://cert.societegenerale.com
Twitter: @CertSG

ABSTRACT

This Incident Response Methodology is a cheat sheet dedicated to handlers investigating on a precise security issue.

1.1.10 WHO SHOULD USE IRM SHEETS?

- Administrators
- Security Operation Center
- CISOs and deputies
- CERTs (Computer Emergency Response Team)

Remember: If you face an incident, follow IRM, take notes. Keep calm and contact your business line's Incident Response team or CERT immediately if needed.

→ IRM CERT SG: https://github.com/certsocietegenerale/IRM

→ IRM CERT aDvens (French version): https://github.com/cert-advens/IRM

1.1.11 6 STEPS ARE DEFINED TO HANDLE SECURITY INCIDENTS

1. Preparation: get ready to handle the incident
2. Identification: detect the incident
3. Containment: limit the impact of the incident
4. Remediation: remove the threat
5. Recovery: recover to a normal stage
6. Lessons learned: draw up and improve the process

IRM provides detailed information for each step of the incident response process. The steps come from NIST Computer Security Incident Handling Guide.

1.1.12 OBJECTIVE: ESTABLISH CONTACTS, DEFINE PROCEDURES, GATHER INFORMATION TO SAVE TIME DURING AN INCIDENT.

Mobile helpdesk must have a defined process in case of a suspected malware infection: replace the smartphone of the user with a new one and isolate the suspicious device for analysis by the forensic investigator.

A good knowledge of the usual activity of the smartphone is appreciated (default and extra tools running on it). A smartphone support expert can be helpful to assist the forensic investigator.

It is recommended to:

- Enable logging (MDM, applications list or else)
- Install Antivirus/Security apps over smartphone
- Configure a VPN to analyze network activity

For Forensic:

- For Android:
  - Activate Developer options with USB Debugging (be careful it could be a risk, public USB charging facilities for example) or have a process to activate it
  - Unlock OEM options if possible
- Test your extraction routines in advance to make sure they are compatible with your evidence

1.1.13 OBJECTIVE: DETECT THE INCIDENT, DETERMINE ITS SCOPE, AND INVOLVE THE APPROPRIATE PARTIES.

Main points of notification for suspicious smartphone:

- Antivirus/Security apps raise alerts
- Check for anomalous rights granted to applications
- Anomalous system activity, unusually slow functioning
- Anomalous network activity, slow Internet connection
- The system reboots or shutdowns without reason
- Applications crash unexpectedly
- User receives one or multiple messages, containing unusual characters (SMS, MMS, Bluetooth messages, etc.)
- Increase in phone bill or web activity
- Calls to unknown phone numbers or at unusual hours/days
- A monitoring should be done to check unusual user bill or network activity

Ask the user about his/her usual activity on the smartphone: which websites usually visited, which external applications are installed.

1.1.14 OBJECTIVE: MITIGATE THE ATTACK’S IMPACTS ON THE TARGETED ENVIRONMENT.

Ask the user to provide his/her credentials to access the smartphone including:

- SIM card PIN code
- Smartphone password
- iCloud login/password
- Google Play credentials,
- backup password…

- Ensure the user is provided with a replacement device to use during the investigation.
- Back up the smartphone data by creating a physical filesystem, logical backup or manual acquisition.
- Put the phone in a faraday bag if available.

After acquisition, remove the battery (if feasible) or put the phone in the airplane mode to block all activity (WiFi, Bluetooth, etc).

Additional actions:

- Remove the SIM to perform additional analysis outside the smartphone.
- Perform an antivirus or security scan of the backup or acquired files on a dedicated forensic station.
- Perform applicable forensic routine base on your use case.

Specific tools should be used by your incident response team to lead forensic investigation on
the smartphone.
Use a dedicated forensic solution to analyze the captured data or the smartphone (Cellebrite, XRY, Oxygen, Axiom, Andriller, etc).

REMEDIATION

1.1.15 OBJECTIVE: TAKE ACTIONS TO REMOVE THE THREAT AND AVOID FUTURE INCIDENTS.

- Remove the identified threat from the smartphone.

Or

- Wipe the infected smartphone and Hard/Soft reset it to factory settings with a pristine firmware.

- Reinsert the SIM card back into the smartphone.

Signal all identified malicious applications still available through marketplaces for

1.1.16 OBJECTIVE: RESTORE THE SYSTEM TO NORMAL OPERATIONS.

- Selectively reinstall saved data and apps from the backup.

You may consider retaining the device for an additional quarantine period to perform appropriate security checks.

For more details on authentication and infrastructure recovery, check the Large-scale malware compromise IRMXXX

LESSONS LEARNED

1.1.17 OBJECTIVE: DOCUMENT THE INCIDENT'S DETAILS, DISCUSS LESSONS LEARNED, AND ADJUST PLANS AND DEFENSES.

Report

An incident report should be written and made available to all of the actors of the incident.

Following themes should be described:

- Initial detection
- Actions and timelines
- What went right
- What went wrong
- Incident cost
- Indicators of compromise

Capitalize

Actions to improve the smartphone policy should be defined to capitalize on this experience.

Debrief the incident with user to improve his/her awareness.