# Infected System Response Playbook

**Table of Contents**

[Infected System Response Playbook 1](#_Toc121336244)

[Document Control 3](#_Toc121336245)

[Revision History 4](#_Toc121336246)

[Distribution List 4](#_Toc121336247)

[Purpose 5](#_Toc121336248)

[References and Document Hierarchy 6](#_Toc121336249)

[Preparation 7](#_Toc121336250)

[Identification 8](#_Toc121336251)

[Containment 12](#_Toc121336252)

[Eradication 15](#_Toc121336253)

[Recovery 18](#_Toc121336254)

[Post Incident Activities 19](#_Toc121336255)

# Document Control

|  |  |
| --- | --- |
| Audience |  |
| Purpose | Policy definition for …….. |
| Document Title | ...... |
| Owner | Head of Technology Services |
| Author | xxxx |
| Date Drafted | xx/xx/xxxx |
| Date Approved | xx/xx/xxxx |
| Information Classification: | Level 1 – Internal |
| Version: | 0.1 |
| Document Status | Draft |

### Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Author | Comments |
| xx/xx/xxxx | 0.1 |  | Initial draft |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

### Distribution List

|  |  |  |
| --- | --- | --- |
| Name | Role | Department |
|  | Head of Technology Services |  |
|  | Cyber & Network Team Leader |  |
|  | Network Manager |  |
|  | IT Manager |  |
|  | Global Service Desk Team Leader |  |

# Purpose

The purpose of the Infected System Response Playbook is to be used as a compliment to the Incident Response Plan. It may also be used in conjunction with the other available playbooks, such as Ransomware Response, and Compromised Accounts Response Playbooks.

The playbook covers the phases from the IR Plan that require additional actions and therefore maintains the same structure.

The sections Scope, Definitions and Incident Response Plan from the IR Plan are equally applicable to this Playbook.

An Infected System may be the result of for example a user browsing to websites, opening attachments from emails, downloading, and executing applications. And although an attacker may not be actively involved in the system compromise, the system may actively be abused by an attacker once the system is compromised.

# References and Document Hierarchy

Reference: Disaster Recovery Framework

Parent document: IR Plan

Children:

* Procedures or technical guidelines

# Preparation

The Preparation Phase from the IR Plan covers all playbooks. Below cover additions specific to this playbook. Reviewing and testing the Infected System Response Playbook should be run at least once a year or following major technical changes.

|  |  |
| --- | --- |
| Step Title | Step Description |
| Backup Strategy | Performing backups of the critical data assets with an adequate data retention period defined, will allow for quick restoration should it be required. The restoration of the backups should be tested regularly to ensure the availability and integrity of the data assets. Offline or immutable backups should be considered to counter malicious activities impacting the backups.  **Responsibility:** Head of Technology Services |
| Exercise Infected System Response Playbook | Run periodic Infected System Response Playbook tests to evaluate familiarity and gaps in the playbook, associated processes, and procedures and in the required skills.  **Responsibility:** Head of Assurance, Risk and Compliance |

# Identification

The goal of the Identification phase is to assess if the incident at hand is in fact caused by an infected system. The incident may already have an initial categorisation and prioritisation attributed to it, which may change after the assessment and consecutive steps.

Diagram

Description automatically generated

Figure Identification Phase

|  |  |
| --- | --- |
| Step Title | Step Description |
| 2.0 Start Identification | Begin the process which would be triggered by an incident being notified from any available source. |
| 2.1 Is it an Event Notification or is it an RFI? | An RFI (Request For Information) always requests to confirm an observed activity and presents recommendations in case the activity is unwanted.  An Event Notification represents any event, any observable or reported occurrence that a preliminary investigation indicates has a sufficient potential for adverse impact on the confidentiality, availability, or integrity of Company’s information technology or data.  Users may report on an Infected System incident as they face unexpected behaviour of the system.  A notification from the 3rd Party Active Response Service (3rd Party MSSP) indicating an Infected System incident will provide recommendations. These recommendations should be implemented when the incident is declared and may overlap with the First Responder Actions.  **Responsibility**: Technical Lead |
| 2.2 Is the Reported Activity Legit? | As part of the RFI, it is requested to confirm an observed activity. If the activity is confirmed to be legit, it must be determined if the event is a false positive.  If the activity is unwanted, the recommendations of 3rd Party Active Response Service (3rd Party MSSP) will be implemented prior to the start and as part of the Containment Phase.  **Responsibility**: Technical Lead |
| 2.3 Event Assessment | Perform initial analysis of the event. Collect additional events related to the event in question.  **Responsibility**: Technical Lead |
| 2.4 Is it an Incident? | If the event is an incident, an incident will be declared.  If the event does not transition into an incident, the event will be evaluated with respect to being a false positive or not.  **Responsibility**: Technical Lead |
| 2.5 Event is a False Positive? | If the event is a confirmed false positive, the 3rd Party Active Response Service (3rd Party MSSP) will tweak the source of the event to avoid future false positives; which is then followed by the Post Incident Activities Phase.  If the event is not a false positive, handle the event as a non-incident event.  **Responsibility**: Technical Lead |
| 2.6 Handle Non-Incident Events | The Event did not transition into an Incident and is not a false positive, yet it may be required to generate these events. This may be required for tracking or reporting purposes.  **Responsibility:** Technical Lead |
| 2.7 Declare an Incident | **Responsibility**: Incident Lead; Technical Lead in absence of Incident Lead |
| 2.8 First Responder Actions | This step would belong to the Containment Phase; however, the following avoids any delays in the initial response to an Infected System incident.  In case the notification was provided by the Active Response Service and not executed by the 3rd Party Active Response Service, the recommendations must be implemented manually.  The 3rd Party Active Response Service provides the capability of quarantining the impacted system. This action both isolates the device and disables the current user account on the device.  Disable any impacted user account not covered with the quarantine capability of the 3rd Party Active Response Service.  Forcefully sign off the account from MS365 services.  Inform the user and the broader IT Team about the actions taken.  **Responsibility**: Technical Lead |
| 2.9 Log and Track Incident | Assign ticket/case number and begin documenting all relevant information in the Enterprise Incident / Change system (Solution).  **Responsibility:** Technical Lead |
| 2.10 Determine Incident Priority | Based on the physical and/or data assets involved, an initial priority can be attributed to the incident. During the analysis and scoping, the priority may change as other physical and/or data assets may be identified as impacted.  **Responsibility**: Incident Lead |
| 2.11 Inform Stakeholders According to the Incident Priority | Communicating with stakeholders is key during an incident. Providing information and setting expectations on the intermediate steps during the investigation, aids stakeholders to steer actions and decisions.  **Responsibility**: Incident Lead, Public Relations |
| 2.12 Specific Playbook is Available? | Additional information from the previous assessment may lead into invoking an additional playbook, for example the Compromised Account Response Playbook or Ransomware Playbook. A specific playbook may be available and would be activated. If no playbook needs to be invoked, the analysis and scoping of the incident will continue to ensure all systems are identified.  **Responsibility**: Incident Lead |
| 2.13 Activate Respective Playbook | Activating and executing the specific playbook addresses the particular activities related to that type of an incident.  **Responsibility**: Incident Lead |

|  |  |
| --- | --- |
| 2.14 Playbook ran Successfully? | At the conclusion of the playbook, it can be determined if the playbook covered the entire incident or grouping of incidents. If that is the case, the process stops. If that is not the case, it should be evaluated if another playbook is available.  **Responsibility**: Incident Lead |
| 2.15 Conduct Generic Analysis and Scoping of the Incident | The generic analysis includes enriching the available information, correlating the information, determining if other functional and/or data assets are impacted etc so to obtain a complete overview and understanding of the incident before taking any coordinated containment actions. Preliminary containment actions may alter the behaviour of the malware.  **Responsibility**: Incident Support/Technical Lead |
| 2.16 Altered Priority? | As the analysis and scoping is performed, additional functional and/or data assets may be identified, leading to a change of the priority.  **Responsibility**: Incident Lead/Incident Support |
| 2.17 Automated Containment? | Determine if any security implementations automatically contained any impacted functional and/or data assets based on applied policies/configuration. If that is the case, the Eradication Phase starts.  The Containment Phase starts if no containment actions are performed automatically or was incomplete.  **Responsibility**: Incident Support/Technical Lead |

# Containment

The Containment phase has the high-level tasks that should be performed to prevent the Infected System incident from growing in scope, impact, and/or priority beyond what has been identified so far. It is done through disruption, degradation, access denial, and/or isolation of the identified asset(s).

Note that some of the activities were performed already on some system(s) during the First Responder Actions step in the Identification Phase.

It is important to note that this phase also aims to preserve as fast as possible the affected data for later forensics activities.

Diagram

Description automatically generated

Figure Containment Phase

|  |  |
| --- | --- |
| Step Title | Step Description |
| 3.0 Start Containment | Continue containing the Incident. |
| 3.1 Isolate | Isolate additional identified affected functional and data assets. This can be performed on the functional asset itself, more granular at the process level or more general at the segment level they are part of.  This step also includes disabling additional affected user accounts.  **Responsibility**: Incident Support, Technical Lead |
| 3.2 Preserve Digital Forensics Evidence | Digital Forensics Evidence is crucial to perform the root cause analysis and essentially learn how the malware got on the system in the first place. If it is a targeted attack, it may learn from the attackers’ procedures and tactics used during the incident. In either case, the security measures can be adjusted to counter similar approaches or patterns in the future. It may also serve if Law Enforcement gets involved.  It should be left at the discretion of the Incident Support to have this step performed as this is not required for each and every Infected System incident, but may primarily be guided by the nature of the involved system.  A forensics investigation benefits from memory images, full disk images or selected disk triage including registry, browser activities, temp folders, logs. These could be taken from both physical or virtual machines, end-user devices or servers. Network related logs are another useful datasource. Consider the firewalls, IDS or any other implemented security measure.  **Responsibility**: Incident Support |
| 3.3 Continue Investigation | Logs and other events should be reviewed accordingly, to ensure adding any additional affected functional or data asset to the scope of the incident.  It will also lead to the generation of Indicators of Compromise (IOCs) that will be used during the next steps.  **Responsibility**: Incident Support |
| 3.4 Additional Assets Affected? | If any additional functional or data asset is identified being affected, it not only becomes part of the scope but also should be isolated in the same fashion.  **Responsibility**: Incident Support, Technical Lead |
| 3.5 Data Exfiltration Occurred? | Relevant parties should be informed if data exfiltration is confirmed. The confirmation stems from indications from the investigation, through ISP volumetric logs, or any other security implementation. Claims from the attacker or notifications from other sources may also confirm data exfiltration.  If it is unclear or it is assumed no data exfiltration occurred, the decision should be made to engage external support or not.  **Responsibility**: Incident Lead |
| 3.6 Activate Data Breach/Data Loss Playbook | The Data Breach Playbook will be invoked as data exfiltration is assumed.  The focus will be on the extent of the exfiltration and type of the stolen data assets through ISP volumetric logs, or any other security implementation providing visibility on outbound network traffic.  The Data Loss Playbook may be invoked if data assets became unavailable as a result from the incident.  External Support may be required to aid with this.  Based on the findings, additional relevant parties need to be informed, which is covered in the Data Breach Response Playbook.  **Responsibility:** Incident Lead |
| 3.7 Playbook ran Successfully? | At the conclusion of the Data Breach Playbook, it can be determined if the playbook covered the entire incident or grouping of incidents. If that is the case, the process stops. If that is not the case, it should be evaluated if external support is required.  **Responsibility**: Incident Lead |
| 3.8 Confident the Incident is Contained? | If the team is confident the incident is contained, the team can move on to the Eradication Phase.  If that is not the case, the investigation should continue.  **Responsibility:** Incident Lead |
| 3.9 Engage External Support | External Support can be engaged to aid in determining the extent of the data exfiltration. They can also be engaged to perform additional forensics, to determine the root cause of the incident, and thereby finding additional IOCs. They may be able to help with other related activities for which does not possess the resources.  External Support is not required if the team is confident the incident is under control and contained.  **Responsibility:** |
| 3.10 External Support Activities | Engaging External Support will introduce a set of actions to be supported and executed prior to leading to the Eradication Phase. Depending on the requested engagement, additional phases may be executed.  **Responsibility**: Incident Lead |

# Eradication

The eradication phase aims to ensure the malware or the attacker is unable to apply changes to the environment, which includes the removal of any deployed malware or unwanted software, a password reset of all affected accounts, the revocation of all abused certificates, the denial of all access avenues to the attacker etc.

To avoid the attacker regaining a foothold in the environment, it is important that the activities in this phase cover all affected assets and are executed in a coordinated, low profile but swift manner. For some incidents, eradication is either not necessary or performed in tandem with the recovery, for example when a segregated clean environment is being built up in parallel to the affected environment.

The timing for executing this phase depends heavily on the accepted risk to have affected assets operational and the ability to confirm the scoping of the incident was executed properly and conclusive.

Diagram

Description automatically generated

Figure Eradication Phase

|  |  |
| --- | --- |
| Step Title | Step Description |
| 4.0 Start Eradication | Begin denying the malware’s ability to function properly or denying the attacker’s access to the environment and revert to a cleaned state. |
| 4.1 Deny Attacker Access and Block Malware Functionality | Block any avenue of access the attacker may have used to access the environment.  Block any functionality for the malware to be installed, executed and function in the environment.  **Responsibility**: Incident Support, Technical Lead |
| 4.2 Disable Accounts | Disable the user and/or system accounts that may have been compromised.  This step and 4.3 Activate Account Compromise Playbook run in parallel with 4.4 Revoke Abused Certificates.  **Responsibility**: Technical Lead |
| 4.3 Activate Account Compromise Playbook | Once the accounts are disabled, turn to the Account Compromise playbook for the additional set of actions. The playbook ultimately includes resetting the credentials.  **Responsibility**: Technical Lead |
| 4.4 Revoke Abused Certificates | If an attacker was able to abuse company issued certificates, VPN, signing etc, revoke those certificates so they are rendered invalid and can no longer be used.  This step runs in parallel with 4.2 Disable Accounts/Reset Credentials and 4.3 Activate Account Compromise Playbook as certificates are managed in a different way and neither have direct impact on each other. This step however, does not necessarily take the same time to execute as 4.2 and 4.3.  **Responsibility**: Technical Lead |
| 4.5 Determine, Store and Apply Relevant IOCs | During or as a result from the investigation, Indicators Of Compromise (IOC) may have been identified. Some may even be particular to and prove valuable for detecting affected assets or attempts to do so. Validate and store those IOCs. Apply the relevant IOCs to the security implementations, such as IPS/IDS, SIEM, AV, blacklists etc. Sharing IOCs with other entities may be considered during or after the recovery phase.  **Responsibility**: Technical Lead, Incident Support, Incident Lead |
| 4.6 Improve Defences | Identify the gaps in the defences that allowed the incident to occur. This may include additional hardening, monitoring, detection, and reporting.  **Responsibility**: Incident Support, Technical Lead |
| 4.7 Rebuild Functional Asset? | Determine if the changes to the functional asset(s) can be reverted or if the functional asset(s) needs to be rebuilt.  **Responsibility:** Incident Support |

|  |  |
| --- | --- |
| 4.8 Clean Affected Functional Assets | Clean[[1]](#footnote-1) the affected functional systems and prepare to rebuild the asset. Cleaning a system refers to applying standard read/write operations to the storage device, such as by rewriting with a new value or using a menu option to reset the device to the factory state.  **Responsibility:** Technical Lead |
| 4.9 Remove Unwanted Software. Eliminate Malware. Restore Clean Configuration | If the functional asset does not need to be rebuilt, remove any unwanted software. It is not uncommon for an attacker to deploy legitimate software, such as remote access tools. Remove malware where possible and make sure all traces are removed. Restore a clean configuration if the IOCs determined changes to the registry or any other configuration.  **Responsibility**: Incident Support, Technical Lead |
| 4.10 Revoke Configuration Changes | It may be that configuration changes were applied not only to individual Functional Assets, but also to the environment as such. These may not be overlooked and should be revoked. The conclusion of this step leads to the start of the Recovery Phase.  **Responsibility:** Technical Lead |

# Recovery

The recovery activities are covered in the IR Plan. No specific additions for this playbook are required.

# Post Incident Activities

The post incident activities are covered in the IR Plan. No specific additions for this playbook are required.

1. NIST Special Publication 800.88 defines *clean* and proposes practical applications depending on the storage medium, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf [↑](#footnote-ref-1)