# MALWARE-OUTBREAK Incident Response Playbook

*Redback Operations*

Document Owner: Purple Team Last Modified By: Devika Sivakumar
Next Review Date: 17 June 2024 Last Modified on: 21 April 2024

| Version | Modified By | Approver | Date | Changes made |
|---|---|---|---|---|
| 0.1 | Devika Sivakumar | | 21 April 2024 | First draft |
| 1.0 | Devika Sivakumar | Joel Daniel | 29 April 2024 | Approved for Publishing |

# Contents

# 1. Introduction

Data integrity, reputation, and company operations are all seriously at danger from malware outbreaks. To reducing harm and guaranteeing business continuity, timely malware incident identification, containment, and mitigation are essential. This playbook offers a systematic approach for managing malware outbreaks, defining roles, duties, and procedures to enable a successful response.

## 1.1 Overview

The incident response playbook for malware outbreaks provides a structured approach to locating, stopping, eliminating, and recovering from attacks by malware. It seeks to expedite reaction efforts and lessen the effect of malware breakouts on organisational assets and stakeholders by creating defined protocols and communication channels.

## 1.2 Purpose

This playbook's goals are to:

- Provide a uniform procedure for tackling malware outbreaks to guarantee consistency and effectiveness in incident management.
- To stop malware from spreading further and to reduce damage, make it easier for occurrences to be quickly detected and contained.
- Reduce the impact of malware outbreaks on company operations and lower the financial losses they cause.
- During incident response activities, encourage cooperation, coordination, and communication amongst response teams, stakeholders, and other relevant parties.

## 1.3 Attack Definition

Malware is software that is intentionally created to cause harm, interfere with operations, or obtain unauthorised access to data, networks, and computer systems. It includes a wide range of dangers, including as trojans, worms, viruses, ransomware, and spyware. Multiple routes, including portable media, malicious websites, email attachments, and software flaws, can lead to malware epidemics.

## 1.4 Scope

The events regarding the malware outbreak on the computers, networks, and endpoints of the company are covered in this playbook. It includes malware problems, both external and internal, that impact stakeholders, data assets, and company processes. This playbook covers all occurrences requiring an integrated effort, regardless of the type of malware or transmission technique.

# 2. Attack Types

Malware outbreaks may take many different shapes, and responding to each one presents different difficulties for incident response teams. Malware outbreaks are often linked to the following attack types:

## 2.1 Worms

Worms are viruses that reproduce themselves and travel around networks, taking advantage of security holes to quickly infect linked computers.

Signs of Worm Activity:

- Unusual network traffic increases, suggesting extensive spreading.
- Worm replication is the cause of the network's rapid bandwidth usage.
- Increased memory or CPU consumption on compromised computers.
- System logs containing files or processes that are unknown.
- Random system restarts or crashes brought on by worm activity.

## 2.2 Trojans

Trojan horses pose as trustworthy applications to deceive users into downloading and running malicious malware, which gives attackers access to infected computers without permission.

Signs of Trojan Infection:

- Suspicious applications or processes running in the background.
- Unusual changes made to files or system settings by Trojan payloads.
- Remote attackers gaining unlawful access to private information or system resources.
- Unexpected toolbar or programme installation on compromised computers.
- Abnormalities in the way the system operates, including sluggishness or frequent crashes.

## 2.3 Ransomware

Ransomware encrypts files or prevents users from accessing their computers, and then demands a fee to unlock the system or restore access.

Signs of Ransomware Activity:

- Files that are inaccessible and have a.locky or.crypt file extension are encrypted.
- Appearance of warning messages or ransom notes requesting money to unlock files.

- Alteration of file dates or properties through the encryption procedures of ransomware.
- Unusual patterns of network traffic as the ransomware talks to the servers that govern it.
- Existence on compromised systems of ransomware-related artefacts, such as executables or registry entries.

## 2.4 Botnets

Botnets are networks of infected devices under the control of hackers, frequently employed to carry out coordinated assaults or disseminate malware payloads.

Signs of Botnet Infection:

- Strange outgoing network connections to command-and-control sites made by compromised devices.
- Large amounts of harmful or spam emails coming from infected computers.
- Botnet activity on compromised devices is causing high CPU or bandwidth utilisation.
- The existence of backdoor trojans or remote access programmes that facilitate botnet communication.
- Unexpected alterations in system behaviour or performance brought on by botnet activity.

## 2.5 Spyware

Without user agreement, spyware secretly records private user data, gathers it, and sends it to hostile parties.

Signs of Spyware Presence:

- Unexpected adjustments to the homepage or default search engine in a browser.
- Display of inappropriate pop-up advertisements or browser reroutes to unsafe websites.
- Existence of toolbars or unusual browser extensions that have been installed without permission.
- Spyware activity might cause a slow internet connection or poor browser performance.
- Criminals gaining illegal access to passwords, surfing history, or sensitive information.

## 2.6 Adware

Without the user's permission, adware gathers user data for targeted advertising, displays invasive adverts, and reroutes web traffic.

Signs of Adware Infection:

- Sudden emergence of unwelcome pop-up advertising or banners when browsing the internet.
- Redirects users who click on links or search results to dubious or harmful websites.
- Adware processes causing slow browser speed or frequent crashes.
- Altering the main page or preferred search engine in a browser without permission.
- Data, database entries, or browser extensions connected to adware being present on compromised machines.

# 3. Stakeholders

Many stakeholders both inside and outside the company must work together and coordinate their efforts to effectively respond to malware outbreaks. In the incident response process, the following parties are crucial:

## 3.1 IT Security Team

The IT security team oversees protecting the company's digital assets, identifying security risks, and putting preventative and corrective measures in place for data breaches. Among their duties and functions are:

- Examining security event analysis to evaluate malware outbreaks' effect and extent.
- Putting security measures in place to stop more illegal access and stop viruses from spreading.
- Working together with the incident response team to control malware outbreaks and reduce their effect.
- Carrying out forensic investigation to find the underlying cause of Malware problems and stop them from happening again.
- Advising on incident response protocols and suggesting security improvements to high management and other stakeholders.

## 3.2 Incident Response Team

The incident response team is responsible for organising cleanup activities and overseeing the organization's reaction to malware outbreaks. Among their duties and functions are:

- Determining the scope and gravity of malware outbreaks and carrying out the required corrective measures.
- Assembling staff and resources to limit and lessen the effects of malware attacks.
- Conducting forensic investigations to ascertain the cause and extent of malware outbreaks and collect data for prospective court cases.
- Communicating incident response protocols and recovery efforts to stakeholders, including top management, outside contractors, and consumers.
- Enhancing the organization's incident response capacity by recording best practices and lessons discovered from malware events.

## 3.3 Communication Team

The communication team oversees overseeing and guaranteeing clear and consistent message for both internal and external communications about malware outbreaks. Among their duties and functions are:

- Creating and implementing communication plans to alert stakeholders about malware outbreaks, such as staff members, clients, and outside vendors.

- Drafting and distributing communication documents to answer queries and concerns from stakeholders, such as press releases, statements, and FAQs.

- Launching media relations and public relations initiatives to safeguard the organization's image and lessen the damaging effects of malware outbreaks.

- Giving the incident response team and senior leadership frequent information on stakeholder involvement and interaction initiatives.

3.4 Customers

Clients are people or groups that have a stake in the goods or services that the company provides and who could be impacted by malware outbreaks. Among their duties and functions are:

- Notifying the company of any unauthorised or questionable conduct pertaining to their accounts or transactions.

- Supplying the incident response team with pertinent data or proof to aid in the investigation of malware outbreaks.

- Following the advice and directives of the organisation on safeguarding their personal information and lessening the effects of virus outbreaks.

3.5 Third-Party Vendors

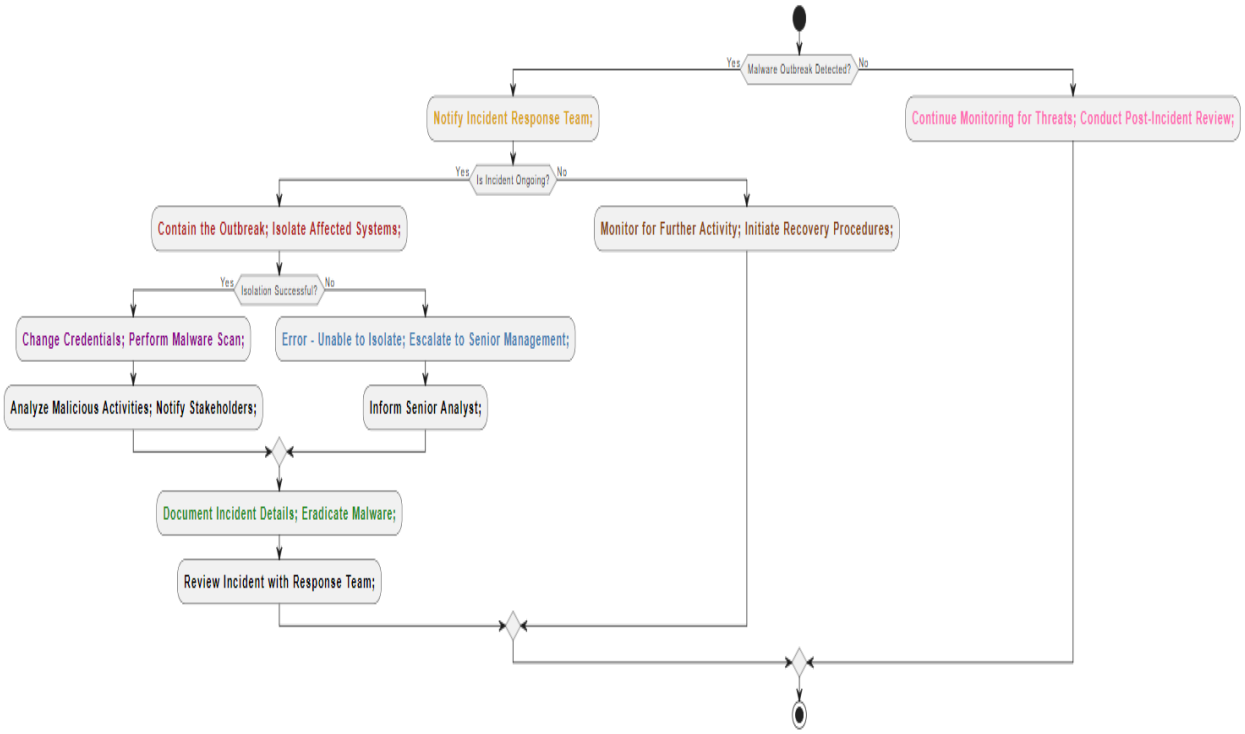
Third-party vendors are outside businesses that supply the company with goods, services, or support; they may also have access to its systems, networks, or data. Among their duties and functions are:

- Working along with the company's incident response team to find and fix security flaws or breaches pertaining to their goods or services.

- Providing help and backing to the company as it investigates and resolves malware problems impacting its systems or networks.

- Meeting legal and contractual standards for data security and privacy, including reporting security breaches, and supporting incident response activities.

# 4. Flow Diagram




1. Preparation (Prep): Yellow

    - Notify Incident Response Team: To begin incident response preparations, the incident response team is notified as soon as a malware outbreak is discovered.

2. Identification (Identify): Red

    - Contain the Outbreak; Isolate Affected Systems: To stop more unauthorised access, steps are made to isolate compromised systems and limit the outbreak.

3. Notification (Notif): Violet

    - Change Credentials; Perform Malware Scan: To mitigate the effect of the outbreak, malware scans and password changes are made.
    - Analyse Malicious Activities; Notify Stakeholders: Malicious activity is found through additional analysis, and stakeholders are informed to plan reaction actions.

4. Containment (Contain): Sky Blue

    - Error - Unable to Isolate; Escalate to Senior Management: Senior management is notified of the issue for resolution if the impacted systems cannot be isolated.

5. Eradication (Erad): Light Green

    - Document Incident Details; Eradicate Malware: To remove the danger, malware removal processes are carried out and incident facts are logged.

6. Recovery (Recover): Brown

    - Monitor for Further Activity; Initiate Recovery Procedures: To restore regular operations, recovery steps are started, and ongoing monitoring is carried out for any new malware activity.

7. Post-Incident Actions (Post): Light pink

    - Continue Monitoring for Threats; Conduct Post-Incident Review: In addition to ongoing threat detection, a post-event evaluation is carried out to assess the response's efficacy and pinpoint areas in need of development.

# 5. Incident Response Stages

## 5.1 Preparation

- **Objective:** Establishing the policies, procedures, and assets necessary to effectively manage malware outbreaks is the primary objective of the preparation stage.
- **Activities:**
  - Assembling an incident response team with distinct responsibilities.
  - Developing crisis response procedures and plans that incorporate communication protocols and escalation pathways.
  - Ensuring readiness by regularly training and practicing incident responses.
  - Putting in place surveillance systems and security measures to find and stop malware outbreaks.
- **Outcome:** A fully prepared business with the ability to respond quickly and effectively to malware outbreaks.

## 5.2 Detection

- **Objective:** The goal of the detection stage is to look for indications of malware outbreaks or illegal access to the networks and systems of the company.
- **Activities:**
  - Keeping an eye out for questionable activity, such strange access patterns, or illegal file transfers, by examining system records and network traffic.
  - Using intrusion detection systems (IDS) and security information and event management (SIEM) tools to find any assaults.
  - Examining anomalies and alerts to distinguish between dangerous and acceptable activity.
- **Outcome:** Early malware outbreak identification enables rapid reaction and mitigation measures.

## 5.3 Analysis

- **Objective:** Finding out and understanding the nature and scope of the malware epidemic occurrence are the main goals of the analysis stage.
- **Activities:**
  - Collecting data and using forensic analysis to identify the source and extent of the malware infestation.
  - Analysing systems and networks that have been compromised to determine attack tactics and the effects on compromised data.
  - Identifying the indications of compromise (IOCs) and strategies, methods, and procedures (TTPs) of threat actors.

- **Outcome:** A comprehensive comprehension of the malware outbreak, considering the causes, effects, and attribution of the outbreak.

5.4 Containment

- **Objective:** The containment stage stops future unauthorised access or leakage of information to mitigate the effect and spread of the event.
- **Activities:**
  - Dividing vulnerable computers and networks to stop attackers from spreading laterally.
  - Putting in place safeguards and access limits to stop illegal access to private data.
  - Containing or obstructing dangerous software, data, or network traffic to stop more harm.
- **Outcome:** Effective handling of the malware breakout incident, minimising the harm done to the organization's data and systems.

5.5 Eradication

- **Objective:** The goal of the eradication phase is to eliminate the attackers from the company's networks and IT infrastructure, along with any hazards or vulnerabilities that may still exist.
- **Activities:**
  - Eradicating bad software and data and returning hacked machines to a safe configuration.
  - Repairing or updating software and systems that are susceptible to attack to stop future exploitation.
  - Examining and amending security procedures and policies to fix any vulnerabilities or faults found.
- **Outcome:** Removing all traces of the malware breakout event and cutting down on vulnerabilities to stop future occurrences of this kind.

5.6 Recovery

- **Objective:** The goal of the recovery stage is to get the affected systems and data back to normal and to start doing business as usual.
- **Activities:**
  - Restoring corrupted systems as well as information backups to guarantee information accessibility and integrity.
  - Rebuilding or rearranging systems and networks to improve security and stop such incidents in the future.

- Putting in place initiatives for user awareness and education to stop malware outbreaks in the future.
- **Outcome:** Complete recovery of services and operations, along with stronger safety protocols to reduce the probability of a repeat.

## 5.7 Post- Incident Review

- **Objective:** The company assesses its reaction to the malware outbreak issue during the post-incident assessment phase, looking for areas for improvements and lessons learnt.
- **Activities:**
- Completing a thorough analysis of the incident response procedure, considering its advantages, disadvantages, and potential areas of development.
- Recording best practices and lessons discovered to improve future incident response capabilities.
- Modifying incident response procedures, policies, and security setups considering the review's conclusions.
- **Outcome:** Enhancing incident response skills and preparing for any malware outbreaks in the future.

# 6. Terminology

- Malware Outbreak: A circumstance in which malicious software quickly spreads throughout the computers, networks, or devices of a company, usually with the goal of stealing, disrupting, or infiltrating data.
- Indicators of Compromise (IOCs): Indications of potentially harmful activity that may be seen in an organization's IT infrastructure and that point to the existence of malware, or a security breech connected to the outbreak.
- Incident Response: A methodical and structured process for locating, controlling, and lessening the damage that a malware outbreak does to an organization's IT infrastructure to reduce interruption and get things back to normal.
- Forensic Analysis: The careful inspection and evaluation of digital evidence associated with the malware outbreak, including system artefacts, malware samples, and network logs, to determine the origin of the attack, gauge its scope, and provide proof for legal or investigative needs.
- Security Controls: Defensive measures and protections, including as firewalls, antivirus software, intrusion detection systems (IDS), and endpoint protection solutions, put in place to identify, stop, and reduce the impact of a malware outbreak.
- Vulnerability: Vulnerabilities or holes in a company's networks, apps, or IT systems that might be used by malware to propagate, get improper access, or do damage. Preventing and managing malware outbreaks requires the identification and patching of vulnerabilities.
- Phishing: A popular attack vector that hackers employ to fool people into disclosing private information, including passwords, usernames, and financial information. This is frequently done through fake emails, websites, or texts. Phishing assaults have the potential to spread malware and start an outbreak of the infection inside a company.