VIRUS-OUTBREAK Incident Response Playbook

Redback Operations

Document Owner: Purple Team Last Modified By: Devika Sivakumar
Next Review Date: 17 June 2024 Last Modified on: 28 April 2024

Version	Modified By	Approver	Date	Changes made
0.1	Devika Sivakumar		28 April 2024	First draft
1.0	Devika Sivakumar	Joel Daniel	29 April 2024	Approved for Publishing

Contents

1. Introduction

The security of data, the continuity of operations, and the reputation of the organisation are all seriously threatened by virus outbreaks. To reduce damage and guarantee company resilience, virus attacks must be promptly identified, contained, and mitigated. This playbook outlines roles, duties, and processes for a successful response, providing an organised method for handling viral epidemics.

1.1 Overview

There is a methodical structure available in the Virus Outbreak Incident Response Playbook for identifying, stopping, eliminating, and recovering from virus attacks. It seeks to expedite reaction efforts and lessen the impact of viral outbreaks on organisational assets and stakeholders by developing defined standards and communication channels.

1.2 Purpose

This playbook's goals are to:

- Create a standardised procedure for handling viral outbreaks to guarantee efficacy and uniformity in event handling.
- Make it easier to quickly identify and confine viruses to stop their spread and reduce harm.
- Reduce the effect of viral outbreaks on the functioning of organisations and the resulting financial losses.
- During incident response efforts, encourage cooperation, coordination, and communication amongst response teams, stakeholders, and other relevant parties.

1.3 Attack Definition

Malicious software, such as viruses, are created with the intent to harm, interfere with, or get unauthorised access to computer systems, networks, and data. They cover a wide range of dangers, such as ransomware, worms, trojans, and spyware, among others. Numerous routes, including malicious websites, email attachments, infected files, and software flaws, can allow viruses to enter a system.

1.4 Scope

Events related to virus outbreaks that impact the computers, networks, and endpoints of the company are covered in this playbook. It covers viral occurrences that affect stakeholders, data assets, and company procedures from both external and internal sources. This playbook is applicable to any situation that calls for a coordinated response, regardless of the type of virus or mode of distribution.

2. Attack Types

There are several ways that virus outbreaks might appear, and each one poses different difficulties for incident response teams. The subsequent assault types are frequently linked to viral outbreaks:

2.1 File Infector Viruses

When executable files are opened, file infector viruses cling to them, multiply, and spread to other files, causing extensive harm.

Signs of File Infector Virus Activity:

- Unknown corruption or alteration of executable files.
- Unexpected variations in checksums or file sizes.
- Reports of malicious file alarms from antivirus software.
- Unexpected rise in system resource consumption brought on by viral propagation.
- Suspicious network traffic coming from machines that have been compromised.

2.2 Macro Viruses

Macro viruses propagate by infecting spreadsheets and documents that include macros. The macros are subsequently performed when the file is accessed, potentially leading to data loss or system interruption.

Signs of Macro Viruses Activity:

- Unusual actions or error messages while attempting to open spreadsheets or documents.
- Emails with links to malicious documents or attachments that seem suspicious.
- Reports of unforeseen modifications to the layout or substance of documents.
- Infected papers are found and quarantined by antivirus software.
- Increased network traffic because of the transmission or sharing of infected documents.

2.3 Boot Sector Viruses

The master boot record (MBR) or boot sector of storage devices can get infected with boot sector viruses, which impair the system's ability to start correctly and may result in data loss or system failure.

Signs of Boot Sector Viruses Activity:

- Anomalous errors during the boot process or the system's inability to boot up. Reports of system files being damaged or missing.

- Notifications from antivirus software that boot sector viruses are present.
- Adjustments to disc partitions or partition tables that are not explained.
- Suspicious behaviour on the network coming from devices that are infected and trying to propagate the infection.

2.4 Polymorphic Viruses

With every infection, polymorphic viruses alter their look and coding structure, making antivirus software's job of detecting and eliminating them more difficult.

Signs of Polymorphic Viruses Activity:

- Files with often changing signatures are identified by antivirus software and placed in quarantine.
- Random crashes or problems on compromised devices that are not explained.
- Reports of unusual or unpredictable behaviour from files or apps.
- A rise in network traffic as the virus looks to infect other machines.
- System logs demonstrating many attempts to run malicious code with different characteristics.

2.5 Resident Viruses

Because resident viruses lodge themselves in system memory, they can continue to function even after the system is restarted.

Signs of Resident Virus Activity:

- Unexpected system lag or deterioration in performance.
- Antivirus software that looks for infections in RAM.
- Persistence in task management or process monitor of processes linked to viruses.

2.6 Multipartite Viruses

Multipartite viruses combine the traits of boot sector and file infector viruses to infect executable files as well as boot sectors, hence increasing their effect and spread.

Signs of Multipartite Viruses Activity:

- Several antivirus notifications pointing to viruses in the boot sector and files.
- System instability or crashes that happen when apps are running, or the system is booting up.
- Reports pertaining to damaged or lost data in the impacted files and storage devices.
- Adjustments to system setups or settings that are not explained.

- Network behaviour suggestive of the spread of viruses via network drives or shared data.

2.7 Network Viruses

By exploiting holes in network protocols or services, network viruses propagate via network connections.

Signs of Network Viruses Activity:

- Abnormal trends in network traffic or sudden increases in network utilisation.
- Warnings from antivirus software that viruses are proliferating over network sharing.
- Identification of questionable behaviour on servers or network equipment.

2.8 Stealth Viruses

To avoid being discovered by antivirus software, stealth viruses hide their existence and carry out their operations. They frequently use sophisticated strategies to stay undetected.

Signs of Stealth Viruses Activity:

- Abnormal trends in network traffic or sudden increases in network utilisation.
- Suspicious behaviour or symptoms, yet antivirus scans show no viruses.
- Unusual modifications to file properties or timestamps that suggest manipulation.
- Anomalies that point to possible illegal access or manipulation in system logs or event data.
- Unusual activity on the network coming from devices that are compromised.
- Reports of anomalous activity or decreased system performance on infected systems.

3. Stakeholders

Many stakeholders inside and outside the organisation must work together to respond to viral outbreaks effectively. Important roles are played by the following parties in the incident response process:

3.1 IT Security Team

The IT security team oversees defending the company's digital assets against virus attacks, spotting security issues, and putting preventative and remedial measures in place. Among their responsibilities and roles are:

- Evaluating the impact and reach of viral outbreaks through the analysis of security event data.
- Putting security measures in place to stop more illegal access and stop the spread of infections.
- Working together with the incident response team to control and reduce the effects of viral outbreaks.
- Carrying out forensic investigations to find the underlying cause of viral occurrences and stop them from happening again.
- Suggesting security improvements and offering incident response procedure advice to high management and other stakeholders.

3.2 Incident Response Team

The incident response team oversees managing the organization's response to viral outbreaks and organising cleaning activities. Among their responsibilities and roles are:

- Determining the extent and intensity of viral epidemics and carrying out the required corrective actions.
- Assembling staff and resources to lessen and mitigate the effects of viral assaults.
- Carrying out forensic investigations to ascertain the origin and scope of viral outbreaks and collect data for prospective legal actions.
- Notifying top management, outside contractors, and clients on crisis response strategies and recovery initiatives.
- Documenting best practices and lessons gained from viral occurrences will improve the organization's ability to respond to issues.

3.3 Communication Team

Regarding viral outbreaks, the communication team oversees making sure that all internal and external stakeholders are informed in a clear and consistent manner. Among their responsibilities and roles are:

- Creating and carrying out communication strategies to alert relevant parties—such as staff members, clients, and outside suppliers—about viral outbreaks.
- Creating and distributing communication materials to answer queries and Concerns from stakeholders, including as statements, news releases, and FAQs.
- Taking part in public relations and media relations campaigns to safeguard the organization's image and lessen the damaging effects of viral outbreaks.
- Delivering frequent reports on stakeholder engagement and communication activities to the senior leadership and incident response team.

3.4 Customers

Clients are people or organisations who depend on the company's goods or services and might be impacted by viral pandemics. Among their responsibilities and roles are:

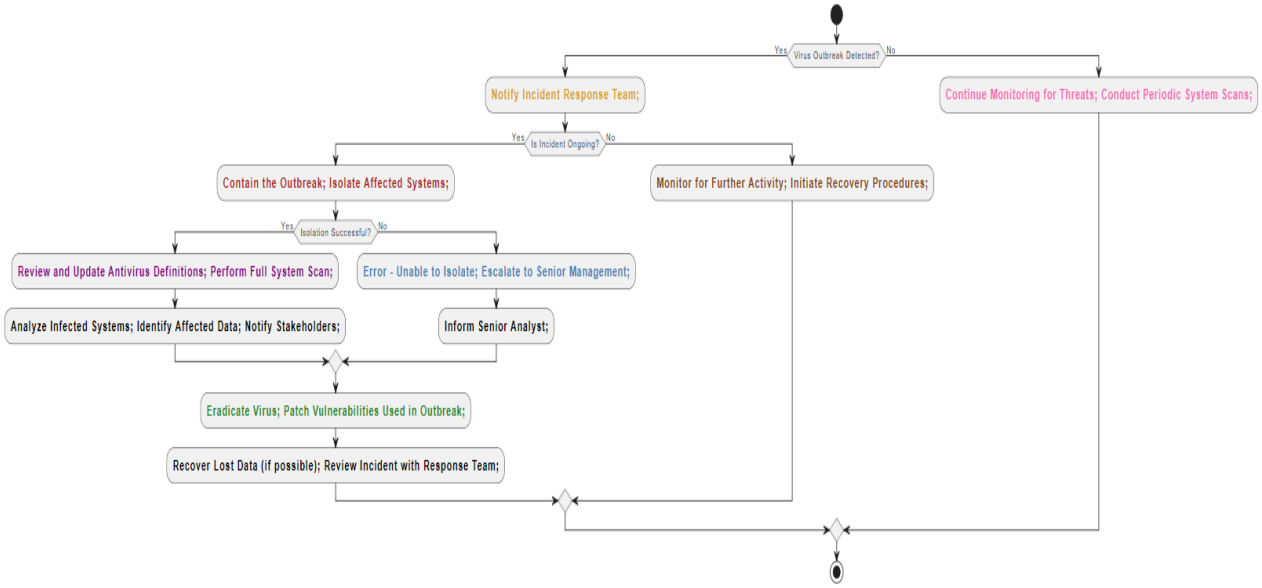
- Notifying the company of any unauthorised or questionable conduct pertaining to their accounts or transactions.
- Supplying pertinent data or proof to support the incident response team's viral outbreak investigation.
- Following the advice and directives of the organisation to safeguard personal data and lessen the effects of virus outbreaks.

3.5 Third-Party Vendors

Third-party vendors are outside companies that supply the company with products, services, or assistance; they may also have access to its networks, data, and systems. Among their responsibilities and roles are:

- Working along with the company's incident response team to find and fix security flaws or breaches pertaining to their goods or services.
- Giving the company help and support while it investigates and fixes any viruses that are damaging its networks or systems.
- Observing the duties imposed by law and contracts on data security and privacy, including the reporting of security breaches and assistance with incident response.

4. Flow Diagram



1. Preparation (Prep): Yellow

    - Notify Incident Response Team: This phase is the first of getting ready to deal with a viral epidemic. As soon as a viral epidemic is detected, the incident response team is informed. We use the colour yellow to represent this stage of preparation.

2. Identification (Identify): Red

    - Contain the Outbreak; Isolate Affected Systems: This phase entails locating the viral outbreak and containing it right away. Measures are implemented to segregate compromised systems and restrict the virus's dissemination. Red is used to represent the vital and urgent nature of this stage.

3. Notification (Notif): Violet

    - Review and update antivirus definitions; perform full system scans: Notifying pertinent parties and putting initial mitigation measures in place are the main goals of this stage. Various measures are implemented to lessen the influence of the outbreak, including altering login passwords, and doing malware assessments. Malicious activity is also examined, and stakeholders are informed so they may organise a response. This notice and early reaction step are represented by the colour violet.

4. Containment (Contain): Sky Blue

    - Error-unable to isolate; Escalate to senior management: At this point, attempts are being done to stop the outbreak's spread. Senior management is informed so that the affected systems may be resolved if they cannot be effectively isolated. The containment measures meant to stop the virus's spread are symbolised by the colour sky blue.

5. Eradication (Erad): Light Green

    - Eradicate Virus; patch vulnerabilities used inn outbreak: The objectives of this step are to eradicate the infection and record incident information. Procedures for removing malware are followed, and incident details are recorded for later use. Light green is used to represent the process of getting rid of the infection and making sure the organization's systems are safe.

6. Recovery (Recover): Brown

    - Monitor for Further Activity; Initiate Recovery Procedures: At this point, attempts are being undertaken to recover from the viral outbreak and get everything back to normal. Recovery processes are started, and continual surveillance is done to find any new virus activity. The recovery phase, which aims to resume regular operations, is symbolised by the colour brown.

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

    - Continue Monitoring for Threats; Conduct Periodic system scans: In the last phase, post-event activities are carried out to assess the effectiveness of the reaction and pinpoint areas that require improvement. A post-event evaluation is carried out to evaluate the organization's reaction to the viral epidemic, and ongoing threat monitoring is maintained. The post-event steps intended to improve future response efforts and learn from the occurrence are indicated by the colour light pink.

5. Incident Response Stages

5.1 Preparation

- **Objective:** Putting in place the tools, processes, and regulations required to control virus outbreaks.
- **Activities:**
  - Putting up a team dedicated to incident response with specific duties.
  - Creating strategies and processes for crisis response, such as escalation routes and communication guidelines.
  - Ensuring preparedness via consistent training and event response practice.
  - Putting security measures and surveillance systems in place to identify and contain viral outbreaks.
- **Outcome:** A well-prepared company that can react to virus outbreaks fast and efficiently.

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 behaviour, such strange access patterns, or unauthorised file transfers.
  - Using security information and event management (SIEM) and intrusion detection systems (IDS) to find and stop threats.
  - Separating malicious from genuine activities by analysing anomalies and alarms.
- **Outcome:** Rapid reaction and mitigating actions are made possible by early virus outbreak identification.

5.3 Analysis

- **Objective:** Recognising the characteristics and extent of the virus an outbreak.
- **Activities:**
  - Gathering information and carrying out forensic investigation to determine the origin and severity of the virus infestation.
  - Examining networks and systems that have been infiltrated to identify attack strategies and the impact on compromised data.
  - Recognising the tactics, methods, and procedures (TTPs) of threat actors and indicators of compromise (IOCs).
- **Outcome:** A thorough comprehension of the virus outbreak, considering its origins, consequences, and sources.

5.4 Containment

- **Objective:** Help lessen the effect of the virus outbreak and prevent more illegal access or data leaks.
- **Activities:**
  - Dividing up susceptible machines and networks to stop intruders from moving laterally.
  - Putting access restrictions and protections in place to stop illegal access to sensitive information.
  - Limiting or preventing harmful data, software, or network flow to stop more damage.
- **Outcome:** Efficient handling of the virus outbreak, reducing harm to the company's information and infrastructure.

5.5 Eradication

- **Objective:** Removing all threats and vulnerabilities from the company's networks and IT systems, including those that still pose a threat.
- **Activities:**
  - Deleting dangerous files and software and putting hacked computers back in a safe configuration.
  - Upgrading or patching susceptible systems and software to stop further exploitation.
  - Examining and amending security guidelines and policies to fix any flaws or vulnerabilities found.
- **Outcome:** Eradication of all evidence of the virus breakout incident and mitigation of susceptibilities to avoid recurrence.

5.6 Recovery

- **Objective:** To restart company operations and return impacted systems and data to normal.
- **Activities:**
  - Restoring damaged systems and data backups to guarantee the integrity and accessibility of data.
  - Rebuilding or rearranging networks and systems to improve security and stop such incidents in the future.
  - Putting user awareness and education programmes into action to stop virus breakouts in the future.
- **Outcome:** Full restoration of operations and services, together with strengthened security measures to lessen the chance of recurrence.

5.7 Post- Incident Review

- **Objective:** Evaluating and pinpointing areas for improvement and lessons gained in the company's reaction to the virus outbreak issue.
- **Activities:**
  - Evaluating the incident response procedure in-depth to find its advantages, disadvantages, and potential areas for development.
  - Recording best practices and lessons discovered to improve incident response skills in the future.
  - Modifying security setups, rules, and incident response protocols considering review results.
- **Outcome:** Improved incident response capacities and preparedness against virus outbreaks in the future.

6. Terminology

- Virus Outbreak: A circumstance in which malicious software quickly spreads throughout the computers, networks, or devices of an organisation, usually with the goal of stealing, interfering with, or breaching data.
- Incident Response: A methodical and organised procedure designed to locate, contain, and lessen the harm a virus outbreak does to an organization's IT infrastructure to minimise interruption and get things back to normal.
- Forensic Analysis: The methodical analysis and assessment of digital data associated with the virus outbreak, such as malware samples, system artefacts, and network logs, to determine the source of the attack, estimate its extent, and supply proof for legal or investigative needs.
- Polymorphic Virus: A kind of virus that is challenging for antivirus software to identify and neutralise as it can alter its appearance or signature with every infection. During virus outbreaks, polymorphic viruses are renowned for their capacity to spread quickly and elude detection by conventional security measures.
- Endpoint Security: A thorough method for protecting mobile, laptop, and desktop computer systems—known as network endpoints—against online dangers including viruses. To prevent virus outbreaks, endpoint security solutions include host-based intrusion detection systems (HIDS), antivirus software, and endpoint detection and response (EDR) technologies.
- Infection Vector: The process or avenue via which a virus enters a network or organisation and infects systems. Email attachments, malicious websites, portable media (like USB drives), and software flaws are frequently used as entry points for virus outbreaks.
- Cyber Threat Hunting: Initiative-taking monitoring and scanning of networks and systems for indications of malicious behaviour or possible virus outbreaks. Cyber threat hunting is the process of identifying and eliminating threats before they become widespread viral outbreaks by examining network traffic, system behaviour, and records.