CMSGu2016-03

National Computer Board

## Mauritian Computer Emergency Response Team

Enhancing Cyber Security in Mauritius

# Guideline on Malware Incident Response

CERT-MU

## National Computer Board
## Mauritius

Version 1.0

July 2016

Issue No. 3

# Table of Contents

***DISCLAIMER:*** *This guideline is provided "as is" for informational purposes only. Information in this guideline, including references, is subject to change without notice. The products mentioned herein are the trademarks of their respective owners.*

# 1.0 Introduction

## 1.1 Purpose and Scope

The purposes of this guideline is to provide process and tasks to help determine the nature of the malware problem, limit the spread of malware, and return the system to operation.

## 1.2 Audience

The target audience for this guideline includes mainly incident handlers and security professionals.

## 1.3 Document Structure

This document is organised into the following sections:

*Section 1* contains the document's content, the targeted audience and the document's structure.

*Section 2* gives a background on malware.

*Section 3* explains the malware incident response design process

*Section 4* concludes the document.

*Section 5* contains a list of references that have been used in this document.

Appendix A consists of a comparison of several malware security products.

# 2.0 Background

Malware or malicious software/code refers to a program that is covertly inserted into another program with the intent to destroy data, run destructive or intrusive programs, or otherwise compromise the confidentiality, integrity, or availability of the victim's data, applications, or operating system.

As the most common external threat to most hosts, malware can cause widespread damage and disruption of organisational information systems and requires extensive recovery efforts by the enterprise.

Unlike malware threats of several years ago, many of today's malware threats are stealthy and quiet, slowly spreading throughout the network, gathering information over extended periods and resulting in loss of sensitive data and other compromises of data confidentiality.

Malware threats can be separated into five broad categories, as follows:

- **Viruses:** Self-replicating code inserts copies of the virus into host programs or data files. Viruses can attack both operating systems and applications.
- **Worms:** A self-replicating, self-contained program executes without user intervention. Worms create copies of themselves, and they do not require a host program to infect a system.
- **Trojan horses:** This self-contained, non-replicating program appears to be benign, but it actually has a hidden malicious purpose. Trojan horses often deliver other attacker tools to systems.
- **Malicious mobile code:** This software with malicious intent transmits from a remote system to a local system. Attackers use it to transmit viruses, worms, and Trojan horses to a user's workstation. Malicious mobile code exploits vulnerabilities by taking advantage of default privileges and unpatched systems.
- **Tracking cookies:** Accessed by many Web sites, these persistent cookies allow a third party to create a profile of a user's behavior. Attackers often use tracking cookies in conjunction with Web bugs.

# 3.0 Malware Incident Response Process

When a malware attack occurs in an organisation, there are a number of factors which must be considered instantaneously to restore service to the system. When deciding which course of action to take to control the attack and quickly restore the system, the following must be considered:

- The amount of time required and available to restore the system to normal operations.
- The resources needed and available to perform the work.
- The expertise and administrative rights of the personnel performing the recovery.
- Any existing policies and procedures regarding incident response within the organisation.
- The cost to the business that could result from data loss, exposure, and/or downtime.

All of these items will influence the decisions and the risk the organisation is willing to accept when responding to and recovering from a malware attack.

The decisions and activities to perform in the malware incident response process are:

- Isolate the threat.
- Notify others to be on alert.
- Gather information about the threat.
- Evaluate the evidence and information gathered about the threat.
- Determine the breadth of the problem.
- Decide the course of action to take: Clean the system, restore system state, or rebuild the system.
- Assess the risk to data, and determine whether the data is backed up.
- Decide whether to examine the root cause of the attack immediately, defer the examination or capture an image for possible legal action, or proceed directly to recover the system.
- Evaluate effectiveness.
- Conduct a post-attack review meeting.

Note that after each action, evaluating the effectiveness of the activities performed will be necessary; because steps may need to be repeated or additional actions may need to be performed to fully reduce the exposure risk to the business from the malware.

Figure 1 provides a graphical representation to confirm an infection and respond to a malware incident.

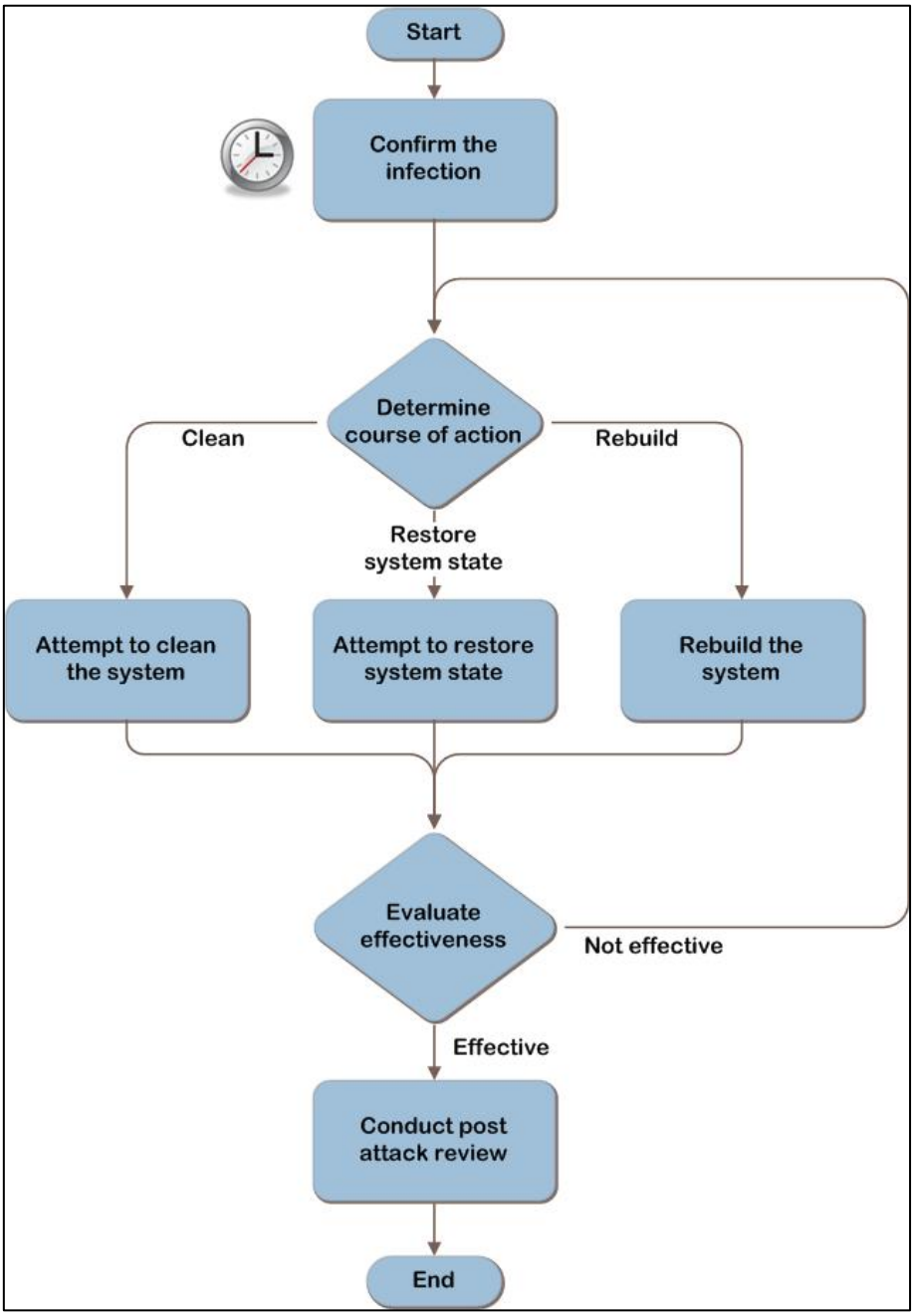


**Figure 1 Response to a malware incident at a high level**

## 3.1 Step 1: Confirm the Infection

This step begins when an organisation suspects a malware infection in the system. This suspicion may have been triggered by a call coming in to the help desk, an alert from the enterprise antivirus system, or some other mechanism.

At this point, it might not be known yet whether it is an isolated incident affecting a single system, an outbreak affecting multiple systems, or a false alarm; however, steps should immediately be taken to contain an infection. Information should be gathered from the user and also about the system to help assess the breadth of the problem.

After completing this step, the collected data should be examined. If evidence shows that a malware incident or outbreak is occurring, continue to Step 2.

The tasks to be performed in this step are:

1. Isolate the threat.
2. Notify others to be on alert.
3. Gather information about the threat.
4. Determine the breadth of the problem.
5. Determine whether malware is present.

Figure 2 is a graphical representation of the tasks to be performed in this step.

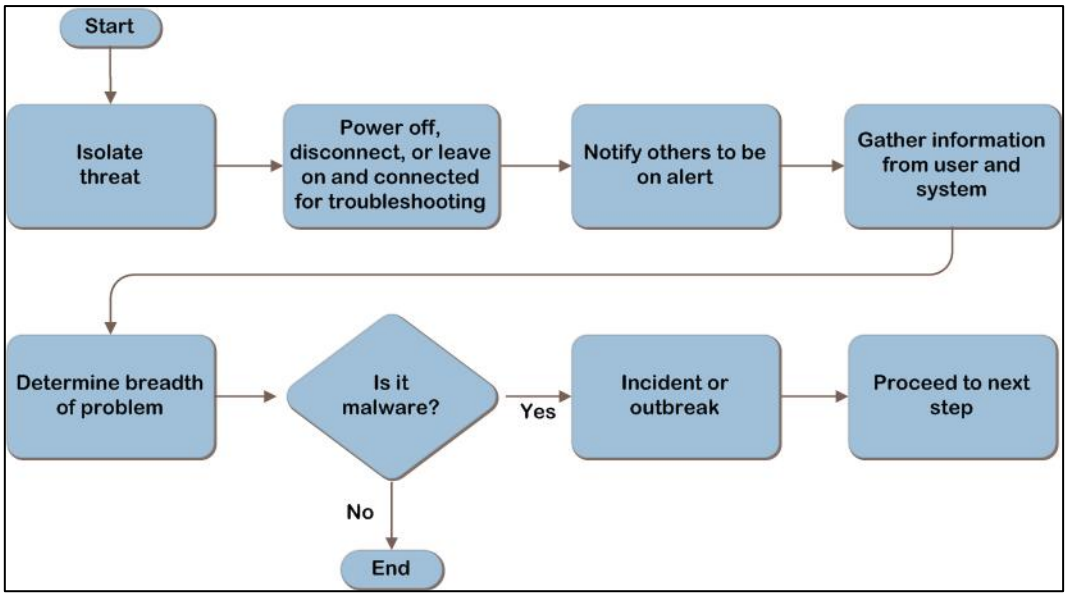


**Figure 2 Confirm the infection**

Although multiple tasks are described in this step, most of the actions will be completed quickly. This step initially assumes that a single incident has been reported, but as additional information is gathered, the scope of the problem and the eventual resolution method may change. For example, a large number of machines infected with a zero-day malware may lead the organisation to begin rebuilding machines in a quarantined network away from potential infection until detection and prevention methods are present.

### 3.1.1 Task 1: Isolate the Threat

When a malware incident is suspected, always assume the worst. First, contain the immediate threat by performing one of the following actions:

- Power the system off.
- Disconnect the system from the network.
- Leave the system on and connected to the network to allow help desk personnel to remotely troubleshoot the system.

Powering off immediately stops the malware's actions and protects individual machines' data not already affected by the malware. This prevents further spread of the malware from this system to other systems in the organisation. This action may be reversed by later decisions, such as using a centrally administered antivirus system to issue a scan command.

A less conservative option is to disconnect the system from the network. This has a potential risk of allowing the malware to continue to be active, possibly destroying data. Network disconnection could be done to individual machines or a portion of the network. If the entire organisation's network is thought to be at risk, access can be severed from the internal network to all external networks.

A third option is to leave the system on and connected to the network to allow help desk personnel to remotely troubleshoot the system. This action presents the risk that the malware may continue to spread to other systems.

The level at which to isolate the problem must be decided quickly to minimize the possibility of infecting other systems. Compare the potential compromise of the system to the risk to the business: the short-term impact of having the system offline and the more long-term potential repercussions if critical data is damaged or exposed outside the company.

Based on the information available, estimate the scope of the threat, and then power off or disconnect systems accordingly.

### 3.1.2 Task 2: Notify Others to Be on Alert

In this task, decide whether to notify other support personnel to watch for an emerging malware outbreak. Time may be an important factor, so the initial responder will be making a judgment call based on the initial assessment relative to the scale of notification. For smaller

IT departments, this may be as simple as verbally asking the other analysts to watch out for other users reporting unusual symptoms. Larger IT departments may have already-defined protocols and escalation procedures that the initial responder will have to weigh against the threat.

If appropriate, notify other support personnel of a possible malware incident so they can be on alert for other reports. Continually gather those reports and add them to the collection of information to help evaluate the scope and severity of the threat. This action informs the response actions in later steps.

#### 3.1.2.1 Validating with the Business

To help understand the organisation's priorities when responding to a malware incident, ask the business stakeholders the following questions:

- **Is there an expectation for the response time required to return the systems to operation?**

  If the business places a high priority on returning the systems to operation, IT may not be able to spend much resource time on determining the cause or source of the infection; all personnel may be needed to rebuild the systems.

- **Have policies and procedures been documented for isolating computers infected with malware so users and the business are prepared for the impact on productivity?**

  Infected systems will be unavailable for use until the malware has been eradicated, and in some cases, the only way to completely remove the malware is to reinstall the operating system and restore the data from a clean backup. Therefore, systems could be unavailable for a significant amount of time.

### 3.1.3 Task 3: Gather Information About the Threat

In this task, information about the threat will be gathered from the user and from the system.

#### 3.1.3.1 Information to Gather from the User

The method used to gather the information below depends in part on whether it was decided to power off or isolate the system. Some of the typical methods of gathering information may be unavailable as a result of efforts to contain the suspected malware, so the person

responding to the incident may need to either witness the symptoms first hand or consult with the user by phone, if necessary.

- **Determine the unusual activity that prompted the report.**
  Although the list is not exhaustive, these are potential types of unusual behaviors that indicate malware may be present on a computer:
    - There is unusual or unaccountable network traffic originating from the computer.
    - The computer runs more slowly than normal.
    - The computer often stops responding to program or system commands.
    - The computer fails and needs to be restarted frequently.
    - The computer restarts on its own, and then fails to run normally.
    - Users cannot correctly run applications on the computer.
    - Users cannot access disks or disk drives on the computer.
    - Users cannot print correctly from the computer.
    - Users receive unusual error messages, pop-up windows, or advertisements.
    - Users see distorted menus and dialog boxes.
    - Users' Internet browser home pages unexpectedly change.
    - Users cannot access administrator shares on the computer.
    - Users notice an unexplained loss of disk space.

- **Get the details of what the user was doing just prior to the unusual activity.**
    - **Determine what may have changed.**
      Even the most seemingly harmless action can produce unexpected results, so ask the user multiple times (perhaps even phrasing it in different ways) whether there have been any changes. For example, new applications were installed, new programs were downloaded, or settings were changed. This gives support personnel a potential direction to pursue.

**Note:** Not every computer experiencing these issues has a malware problem. Misconfigured applications, software bugs, or malfunctioning hardware can also cause such issues.

### 3.1.3.2 Information to Gather from the System

Gather information from the system to help understand the nature of the issue as well as to help determine the breadth of the problem (this will be described in more detail in Task 4).

If the system is still powered off to contain the malware, the information in the list below may be obtainable from management systems such as the antivirus software's administrative console.

**Note** Use care if powering the system back on - doing so may reactivate the malware.

- **Determine whether antivirus and antimalware software was installed, running, and up to date.**

  If all answers are yes, then there may be less reason for worry, because it is more likely to be a malfunctioning system rather than malware. However, if it is indeed malware and the system is up to date, this may indicate that the malware is unknown (new, zero-day, or targeted malware), and cleaning options are not available, yet. This information will be applicable in Step 2.

- **Determine whether all updates and patches for the operating system and applications were current.**

  An out-of-date system is more likely to be compromised, as known vulnerabilities have been disclosed and patches released.

Record the date and time the incident was reported, along with a description of the suspicious behavior.

### 3.1.4 Task 4: Determine the Breadth of the Problem

Determine whether this is an isolated incident or multiple systems are experiencing the same problems.

- Is the user who originally reported the problem aware of others having the same problem?
- Are there an unusual number of reports within a designated timeframe?

Reports that other users are having the same problem may increase the alert level, because it might indicate an outbreak rather than just an isolated incident.

Determine the scope of the suspected malware. The scope may be adjusted as new information is obtained.

### 3.1.5 Task 5: Determine Whether Malware Is Present

Evaluate the evidence to determine whether the organisation is indeed experiencing a malware attack. Reasonable suspicions of malware include:

- Antimalware software reporting via a message that malware was detected during either a real-time detection or a full system scan.
- Unusual behavior of computers consistent with known types of malware disruption that cannot be explained by system malfunction.
- Symptoms that are getting worse on a system.
- Symptoms that are spreading to other systems.
- Symptoms consistent with “in the wild” reports.

Perform an Internet search and check security vendors’ websites to see whether there are reports “in the wild” with the same symptoms and a remedy will be available in the near future. If so, the ability to quickly clean the system may be possible. But if it appears that the remedy will not be ready quickly enough for the system to return to service because of business needs, then the computer will need to be restored or rebuilt. This will be described in more detail in Step 2.

Before triggering an incident response plan, determine whether the incident meets the organisation’s predefined thresholds, if they exist. Consider whether the characteristics or severity of the attack symptoms warrant initiating the incident response plan.

After examining the data gathered from the incident report, decide whether a malware incident or outbreak is occurring. If it is likely that there is an infection, continue to Step 2.

## 3.2 Step 2: Determine Course of Action

In the previous step, actions were taken to immediately contain an infection, and information was gathered about the unusual behavior reported. A determination was made on whether the incident was an actual issue, and if confirmed, others were notified to be on alert. In addition, the scope of the problem was defined to assess the impact in the organisation.

In this step, the decision is made about whether to clean, restore system state, or rebuild the computer. There are often many competing factors to consider when choosing an approach to take to remove malware from a system. To optimise the approach for successful removal of

the malware, all factors must be considered together and a risk tolerance decision made. Items to consider include:

- **The difficulty of the recovery.**
  - What personnel are available to assist with the effort, and what expertise or administrative privileges will be required?
  - Can the issue be resolved remotely, or must it be done by someone onsite?

- **The urgency in returning the system to service.**
  - Is it more important to stop the malware or remove the malware?
  - Is restoring the system to service quickly the most important thing, or is the system not useful until all of the data is restored?

- **The risk to the organisation if a compromise is made between speed and guaranteed removal.**
  - Which is more important: the time it will take to recover the system or the quality of the recovery?
  - If the decision is to restore the system to a state before the malware attack, what is the risk tolerance to the business if traces of the malware remain or security settings have been changed?

These factors must be weighed against the scale of the threat and the level of automation in the organisation.

The remaining steps in this guide are generally written to recover a single system, but the principles are the same to recover from an outbreak, as well. The tasks to be performed in this step are:

1. Determine the risk to data.
2. Decide whether to examine the malware's effects on the system.
3. Decide whether to clean, restore system state, or rebuild.

Figure 3 shows the steps to be performed when deciding which course of action to take.

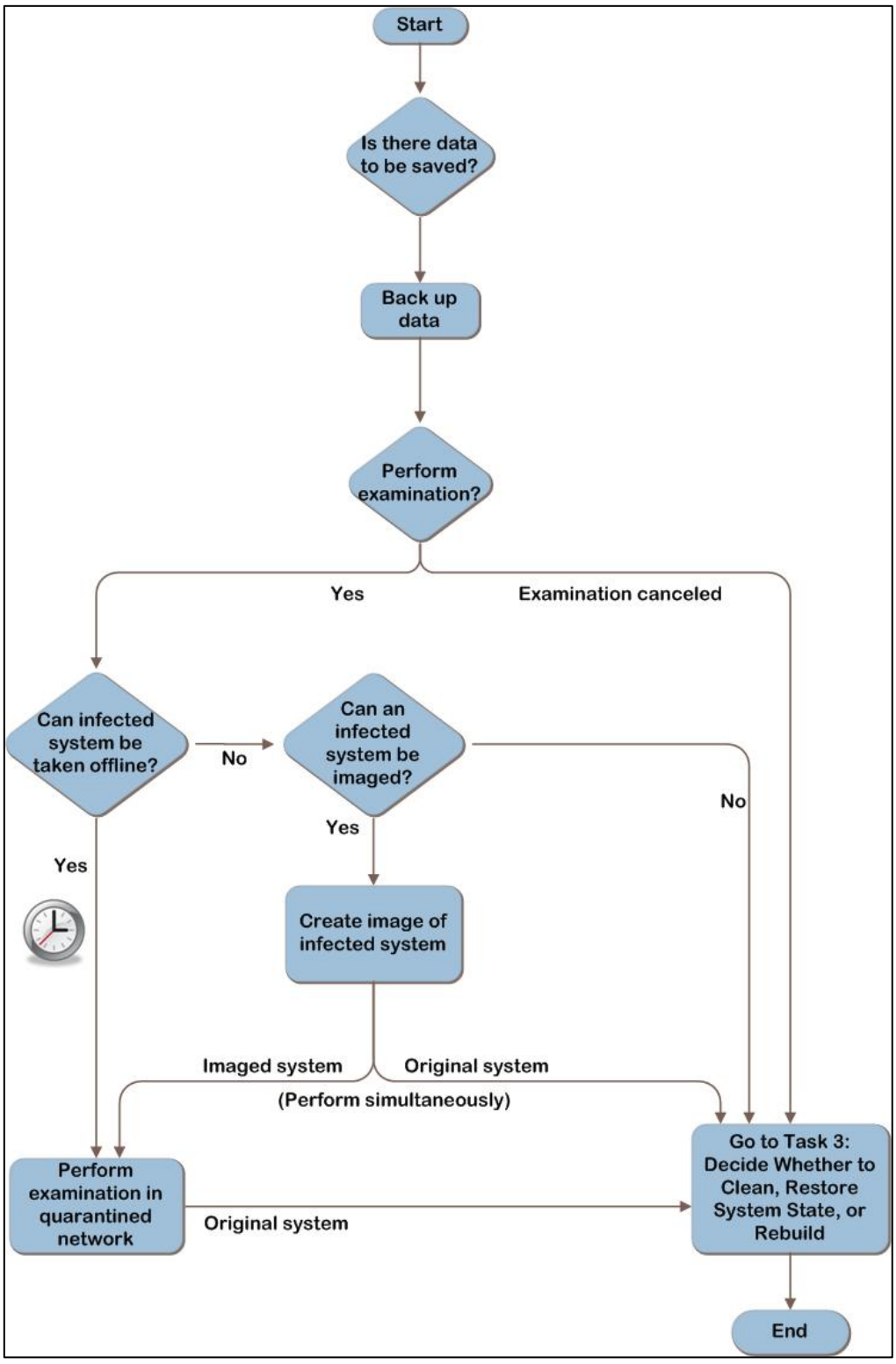


**Figure 3 Determine the course of action**

The clock icon in Figure 3 indicates that there might be constraints on the amount of time spent examining a system taken offline. If the time the business can allow for examination is

exceeded, the efforts to examine might be abandoned so the system can be recovered or rebuilt and returned to service.

### 3.2.1 Task 1: Determine the Risk to Data

The most valuable asset is most likely the data that resides on the system. As a result, it is crucial to consider the risk to the data and verify whether the data has been backed up.

Questions to ask are:

- Is there data on the computer that is important to save?
- Does the computer or any devices attached to it contain mission-critical data? Consider the following:
    - Operating system files and the configuration settings required to restore the host operating system to its original state so all services are functioning correctly.
    - Application installation sources, configuration settings, and data.
    - User data**,** such as documents and spreadsheets, email, and user profiles.

**Note** Depending on when the system was infected, the backed-up data is at risk of being infected, as well. Be cautious when working with this data until a reliable method of checking the data for the malware has been identified.

Alternatively, classifying machines according to their basic profile may allow faster evaluation of the risk to data. For example, the affected machines could be categorised as follows:

- **A system containing no data and performing non-critical functions, such as a kiosk.**

  This profile will be simple to rebuild and less time-critical to return to operation.

- **Systems that serve a critical, time-sensitive function, such as a point-of-sale system or a shop floor automation computer.**

  These systems will have a priority to return to service.

- **Systems with complex application configurations or other complications.**

For example, the source software to reinstall an application or an image of the system is not available. When determining the course of action in Task 3, rebuilding will be a last resort.

- **Systems with critical data that have not been backed up.**

#### 3.2.1.1 Back Up Data

If it is determined that data on the system needs to be backed up, back up the data now or leave the computer powered off until it can be backed up. Consider using offline mechanisms to back up the data. If backups are made with the infected operating system running, the malware may continue to infect or destroy the data.

Verify that the backup is successful to ensure that the entire set of data can be restored and that it is not infected.

**Note** The time taken to attempt removal of the malware (or just having the computer powered on) could result in continued data corruption or destruction from the malware.

### 3.2.2 Task 2: Decide Whether to Examine the Malware's Effects on the System

Decide whether the organisation wants the malware's effects on the system examined. Examination can be beneficial to the organisation to determine who, what, where, how, and why the infection occurred; however, it also takes time and expertise to perform. Performing this examination is optional; the organisation may decide that it is not important to know the details about the malware infection.

The primary factors when considering examination are whether the organisation has the expertise needed and how urgent it is to return the system to operation.

Ideally, the processes of system recovery and examination should be run in parallel to ensure the fastest possible recovery time. The following describes two potential options for obtaining a system for examination:

- The symptomatic system can be examined. Note that the system will need to be out of service during the time that it is being examined, so this may delay its return to service. If multiple systems are affected, a single symptomatic system can be pulled

aside and used for examination, with steps performed in parallel to return the others to service.

- A symptomatic system can be kept offline long enough to create a virtual image of the system for examination. Time spent imaging the system delays its return to service, but this may be quicker than examining the system on the spot.

If it is determined that there is sufficient time, the effects of the malware on the system can be examined. Otherwise, if the business requires the system be returned to operation as quickly as possible; continue to Task 3 to determine the best way to do that.

**Important** If it is decided not to perform the examination, basic information such as information recorded in Step 1, Task 3 should be retained. It is difficult to determine which other systems, backup media, or removable media were possibly exposed to the attack without this information.

### 3.2.3 Task 3: Decide Whether to Clean, Restore System State, or Rebuild

Decide whether to attempt to clean the malware, restore system state, or rebuild the system. Note that cleaning and restoring system state are not always successful, in which case rebuilding is the last resort.

Choosing which option to use should depend on the organisation's level of confidence that the option selected will reduce the malware risk to a level the organisation is willing to tolerate.

Factors to consider when making this decision include:

- How many systems are affected?
- Is there a documented way to remove the malware? If not, does the organisation have the time to wait until directions are available from antimalware vendors?
- Can the recovery processes be performed with minimal or no hands-on work, or do they involve hands-on work by an onsite technician?
- How long will it take to recover the affected systems? If rebuilding the system, are there images of the systems and are the computers' configurations well documented?
- Is there enough confidence that the system can be cleaned or restored to a known good system state? If not, does the organisation prefer that IT to go straight to rebuilding the systems?

- What expertise and administrative rights will be required, and do personnel performing the work have them?

At a high level:

- Cleaning removes the malware but does not restore system settings and files. This is generally fast and can be done locally or, in some cases, remotely.
- Restoring system state restores system settings and files, which typically disables the malware from running but does not necessarily remove malware from the system. Restoring a system must be done manually at each system and is generally fast.
- Rebuilding the system is the only method that ensures that the system will not have malware. The operating system is completely reinstalled, and then user files and settings are reloaded. Depending on the organisation, this can be done locally or remotely. It is, however, the most time-consuming and complex solution.

Table 1 provides more detail on the advantages and disadvantages of each option.

| **Method** | **Pros** | **Cons** |
|---|---|---|
| Clean | • Generally simple and fast process, if cleaning tools are available.<br>• Best chance of keeping the applications and data intact.<br>• Some malware can be cleaned by triggering a scan from a central administration console. | • Exact variant of malware must be known and removal process available from antimalware vendors.<br>• Removes malware but does not restore system settings and files.<br>• Might not completely eradicate malware, or there could be undetected secondary infections. |

| | | |
|---|---|---|
| Restore system state | • Restores system settings and files to a previous known good point in time.<br>• Less destructive than rebuilding the system.<br>• Generally fast process. | • Does not necessarily remove malware—may only inactivate it.<br>• Requires that a backup or restore point be created before the malware incident took place. If it is unknown when malware infected the system, backup or restore points cannot be trusted.<br>• May not be scalable to large numbers of computers unless it can be automated. |
| Rebuild | • Provides the highest degree of assurance of eliminating the infection or attack. | • More complex process, especially if a backup and recovery solution is not in place prior to the infection. |

**Table 1Pros and Cons of System Cleaning, Restoring, and Rebuilding**

**Note** If the decision is made to clean an infected system, the organisation's management and legal teams should perform a risk analysis to determine whether they are willing to accept the increased risk if the cleaning process misses part of the malicious code. For example, it is possible the missed malware may cause the system to be more susceptible to future attacks or make its way into files or software shared outside the company, affecting reputation, revenue, and resources.

If attempting to clean the virus, continue to Step 3. If attempting to restore system state, go to Step 4. For information relative to rebuilding the computer, go to Step 5.

### 3.2.3.1 Validating with the Business

To ensure that all requirements have been identified to recover from a malware incident, ask business stakeholders the following questions:

- **Does the recovery plan budget resources appropriately, depending on the scope of the outbreak and the business impact of the affected computers?**

  In many cases it will be quicker to rebuild systems than to try to remove complex malware; however, a system with critical business data may be worth the time and

effort required for removal, especially if no current data backup is available for the affected systems.

- **Are there different response expectations to address different types of data and systems, such as High Impact, Medium Impact, and/or Low Impact designations for these different assets?**
  The response speed may vary relative to the importance of the affected systems. For example, the response time would be much quicker when an email server has been infected with malware than when an informational kiosk in a building lobby has been infected.

## 3.3 Step 3: Attempt to Clean the System

In the previous step, questions were asked to determine the risk to the data, and the data to be backed up was identified. A decision was made whether to examine the malware's effects on the system. Then, it was decided whether to clean the malware, restore system state, or rebuild the system. If it was determined in Step 2, Task 3 that attempts will be made to clean the system, follow the tasks in this step.

The system might be able to be cleaned by running online or offline scans, using specialized tools, or manually cleaning the system. Multiple methods may be needed to clean the system, and information will be presented to assist in determining which methods should be used. After performing each task, evaluate the effectiveness. If the malware is particularly resistant, it could be that none of the methods is effective; performing a restore or rebuild might be the only remedy.

The tasks to be performed in this step are:

1. Clean the system.
2. Evaluate effectiveness.

When the malware can no longer be detected, update the operating system and applications with the latest patches available from their respective vendors.

Figure 4 provides a graphical representation of the tasks to be performed in this step.

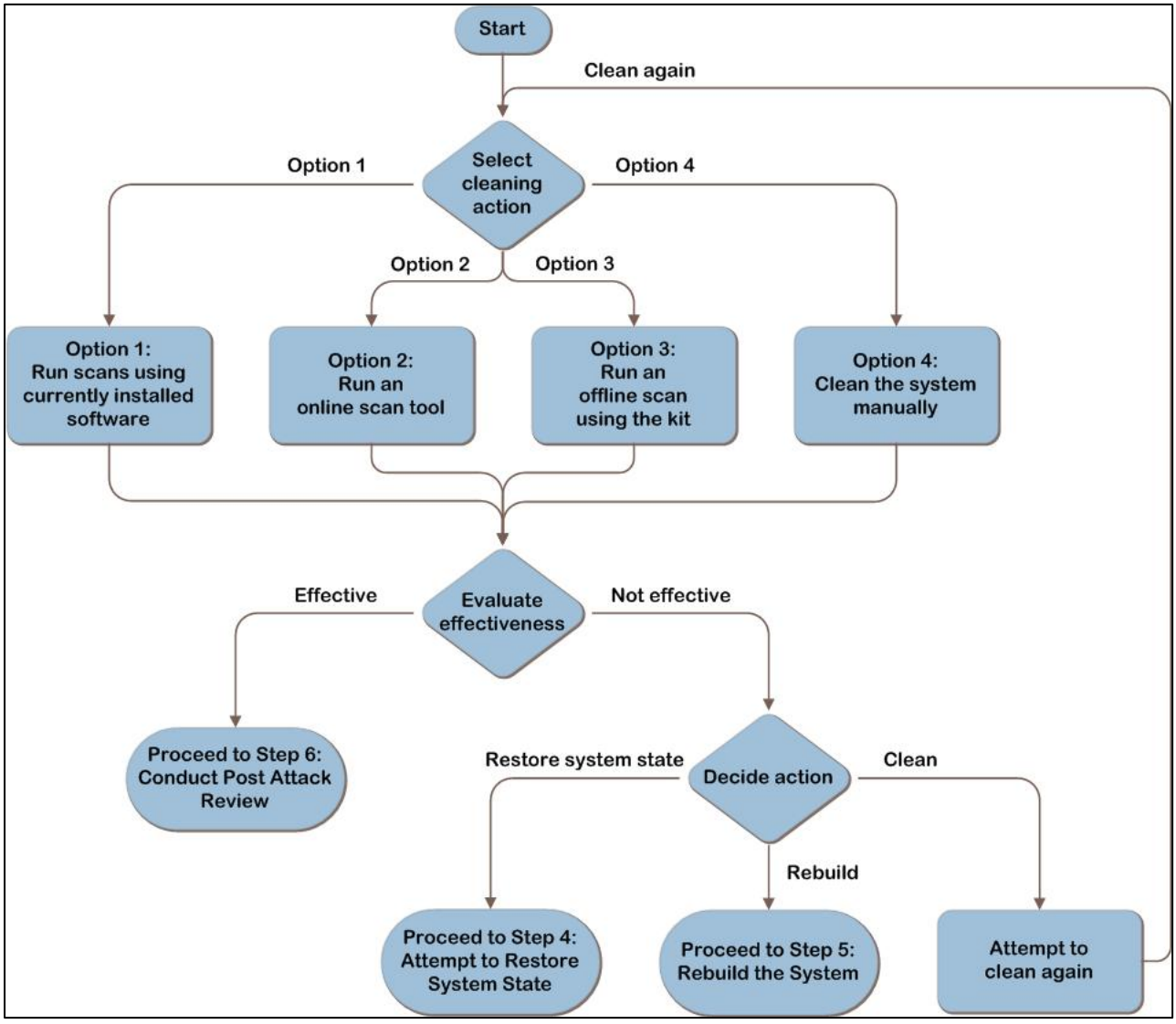


**Figure 4Attempt to clean the system**

### 3.3.1 Task 1: Clean the System

Use scanning tools to detect and potentially automatically remove any malware from the system, or manually remove the malware. The options below are listed in order of ease of execution. Consider the first option and then move progressively to more intensive attempts until the organisation is confident the malware issue is resolved.

The cleaning options are:

- Use locally installed antimalware software with updated signatures, with the operating system started normally and/or in safe mode.
- Use online scan tools, with the operating system started normally and/or in safe mode with networking support.

- Run an offline scan using the offline scan kit.
- Manually clean the system.

The first three options require starting the computer into its installed operating system, which involves risk.

Because it is possible that starting the operating system (even in safe mode) will allow the malware to continue its destructive course, it is important to ensure that data has been backed up (as described in Step 2, Task 1). If there is data on the system, the malware may corrupt or destroy it. Consider powering on the system in a network quarantined from the organisation's main production network so the malware does not spread. There are multiple ways to accomplish this, such as a quarantined physical network, a firewalled network, or another network quarantined logically with rules to restrict the traffic.

In addition, some malware is capable of concealing itself from the scanner. The malware may prevent the antimalware software from being installed, updated, or launched.

If the organisation does not accept the risk of starting the system into its operating system, then use the offline scan kit described in Option 3 in this task.

Conversely, although offline scanning is an effective method for removing many kinds of malware, it does have limitations. Using a combination of methods and/or antimalware products may be used to further mitigate the risk.

#### 3.3.1.1 Option 1: Run Scans Using Currently Installed Software

The first option is to use the locally installed antimalware software to scan the computer. A user can trigger the scan with guidance, but some tasks, such as attempting to remove malware detected by the software, could require administrative privileges.

Locally installed software may not have been protected against the initial infection, but if it is a new strain of malware and signatures have since been released, the software may be able to detect and remove the malware now.

Always verify that the most recent signatures are installed on the computer. Because the system may have been moved to a network with no Internet access to keep the malware from

spreading, manually updating the signatures by downloading them on another computer and transferring them via mechanisms such as USB key may be required.

If the organisation accepts the risk, running a scan using software that is already installed is faster than installing and scanning with other antimalware software. Attempt to detect and clean the malware with the locally installed antimalware software with the system started normally; or, to accelerate the process, start the system in safe mode to perform this option.

#### 3.3.1.2 Option 2: Run an Online Scan Tool

The second option is to run an online scan tool. Online scanning tools allow use of different engines to attempt to detect the malware. However, they require Internet access and may require installation of Microsoft ActiveX® controls or web browser add-ons. Users may require administrative rights on their systems to install these. Only install ActiveX controls or add-ons if the publisher and the website offering them are trusted. In addition, note that online scan tools do not provide real-time protection and cannot be triggered to run automatically across a number of computers.

As mentioned previously, running scans in safe mode may produce better results than a normal start. Because online scan tools require Internet access, safe mode with networking support should be selected.

**Note** Certain malware can edit the Hosts file so that when a user attempts to access a certain legitimate website, the browser is instead redirected to a malware site. Manually cleaning the Hosts file may restore access to online scan websites.

#### 3.3.1.3 Option 3: Run an Offline Scan Using the Kit

When using an offline scanning kit, the computer is started from the CD-ROM, DVD, USB device, or network, and then offline scanning tools are used to repair the primary hard disk drive while it is offline. Using this method, the hard disk drive on the computer is not used to start the computer or scan it, and thus files on the hard disk will not be locked by the operating system. The offline scan then can attempt to access and remove malware that has altered or corrupted these normally locked system files.

Because it requires a start from a source other than the regular boot partition, this method may require sending a technician to the site. In addition, the offline scanning kit will need to be created.

A disk cannot be scanned for malware if it has been encrypted with an encryption tool if the disk is managed as part of a redundant array of independent disks (RAID) volume created with Windows Disk Management or if the disk is damaged. In these cases, or if the person performing this task is unsure of the state of the disk, consult a specialist to determine its state.

#### 3.3.1.4 Option 4: Clean the System Manually

Consider manual system cleaning only if the attacks and behavior of the malware are well documented and the cleaning procedures have been tested and proven. These procedures generally become available to address major viruses or worms.

Sometimes security vendors release specialised automated tools, separate from the antimalware software, for cleaning specific variants. These specialised tools can be an efficient method of cleaning and may reduce errors or missteps, but they are not developed for every variant.

Manual cleaning can be complex and time-consuming. It requires a detailed understanding of how operating systems work and significant expertise about malware.

**Examples of free tools that can be used to clean the system manually**

- Microsoft Safety Scanner at **www.microsoft.com/security/scanner/en-us/default.aspx** is a free downloadable security tool that provides on-demand scanning and helps remove viruses, spyware, and other malicious software. It works with existing antivirus software.

- The Windows Sysinternals tools, such as Process Explorer, Autoruns, and RootkitRevealer at **http://technet.microsoft.com/sysinternals**, can help uncover malware, including malware that attempts to hide itself on computers.

The high-level steps to manually clean malware from the system are:

1. Stop the malware execution processes. Any currently running malware-related process must be terminated as well as any auto-run entries, startup items, or scheduled tasks associated with the malware. Malware that blocks the launching of Task Manager or Process Explorer can pose a challenge.
2. Remove the introduced malware files. This requires a detailed examination of the files on the host hard disk drives to determine which files were affected by the malware.
3. Undo any other system changes the malware introduced, such as restoring the local Hosts file and firewall configurations on the computer.
4. Apply the latest security updates or patches to mitigate the vulnerabilities the original attack exploited. This may require a number of restarts and visits to the Windows Update website or non-Microsoft application vendor sites to ensure that all security updates are applied.
5. Change any passwords (domain or local) that may have been compromised or that are weak and easily guessed.
6. Restore user files modified or deleted by the malware.

If the decision was made to manually clean the system, use the steps described above as a remedy for the infection, and then compare the steps taken with published cleaning procedures as soon as they are available. This will ensure all of the necessary steps have been performed.

Table 2 provides more detail on the advantages and disadvantages of each option.

| Method | Pros | Cons |
|---|---|---|
| Option 1: Run scans using currently installed software | • May be initiated by a user with guidance or remotely from an administrative console.<br>• Faster than other methods, because it uses already-installed software. | • Some remediation tasks may require administrative privileges.<br>• Definitions must be updated to include detection for the malware (assuming that original real-time protection did not detect the malware).<br>• Requires starting the computer into its installed operating system, which could allow malware to continue its course. |
| Option 2: Run an online scan tool | • Allows the use of different engines to attempt to detect the malware. | • Requires Internet access and may require installation of ActiveX controls or web browser add-ons.<br>• Requires starting the computer into its installed operating system, which could allow malware to continue its course.<br>• Cannot be triggered to run automatically across a number of computers.<br>• Does not provide real-time protection. |

| Method | Pros | Cons |
|---|---|---|
| Option 3: Run an offline scan using the kit | • Higher confidence in malware removal; does not use the currently installed operating system to start, thus files on the hard disk are not locked by the operating system so malware can be removed from them. | • Requires a start from media, so may require sending a technician to the site.<br>• An offline scanning kit must be created.<br>• Some disks cannot be scanned for malware, such as those that have been encrypted with a tool such as BitLocker, are part of certain RAID volumes, or are damaged. In these cases, consult a specialist. |
| Option 4: Clean the system manually | • May be faster if malware is well documented and cleaning procedures are available.<br>• Some antimalware vendors release specialised cleaning tools. | • Requires starting the computer into its installed operating system, which could allow malware to continue its course.<br>• Not all malware is well documented.<br>• Can be complex to perform. Requires a detailed understanding of how Windows operating systems work and significant expertise with malware. |

**Table 2 Pros and Cons of System Cleaning Methods**

### 3.3.2 Task 2: Evaluate Effectiveness

At the end of each option, evaluate the effectiveness and consider whether additional measures, including rerunning scans, need to be taken to ensure that the system can be safely returned to production.

Evaluate the effectiveness of the attempts to return the system to service:

- **Does it appear that malware is still on the system?**

It is important to note that a scan returning a result of "no malware found" does not conclusively mean there is no infection. Signatures may not be available from the vendor yet to detect the malware if it is a new strain, or the malware may be concealing itself. Because of the ever-changing nature of malware, no process can be considered 100 percent effective for cleaning malware from a computer. It may be necessary to perform more than one or even all of the options. Manual cleaning steps, described in this task, also may need to be performed in addition to the scans.

- **Are there any security or system settings that are not corrected?**
  Even if the malware can no longer be detected, it might have made other modifications, such as to permissions or accounts that need to be detected and addressed. Review the malware information provided by the security vendor and determine whether additional steps need to be taken. If the malware's effects are not well documented in terms of all changes to the system, rebuilding is the only option to return the system to a known good state.

If the organisation has an antimalware support team, it will need to ensure that the inspection and remediation procedures used to identify and mitigate all possible attack vectors are adequate. Failure to ensure that the procedures are adequate could lead to a rapid reinfection.

If the organisation is confident that the malware is under control on this system and all concerns have been addressed, then the remediation steps can be applied to any other affected systems. If malware appears to still be causing issues after attempts to clean the system, there are two options to consider:

- Attempt to restore system state (see Step 4).
- Rebuild the computer (see Step 5).

## 3.4 Step 4: Attempt to Restore System State

If it was decided in Step 2, Task 3 to restore system state, continue with the tasks in this step. This step makes an attempt to restore system state from backups. This is less destructive than rebuilding the system by completely restoring the operating system but may not be scalable to large numbers of computers unless it can be automated.

As a reminder, any critical data that is on the system should be backed up as a precautionary measure. See Step 2, Task 1 for more information.

**Note** Because virus signature files are released regularly, a restore that failed days before could succeed now (after the antimalware application is updated). Conversely, if the system is restored to a point that succeeded before but a new signature file enables detection of an attack on a backed-up file that cannot be cleaned, the restore process might fail.

The tasks to be performed in this step are:

1. Restore system state.
2. Evaluate effectiveness.

### 3.4.1 Task 1: Restore System State

This task uses tools to restore the operating system files back to a point before the malware affected the system. Restoring the system state does not remove files from a system, it returns any system or application files to a previous state, effectively disabling the malware. Cleaning tools may need to be run after this step to remove the inactive malware.

The tools for restoring the system state vary depending on the installed operating system, but the mechanisms are similar.

The tools protect critical system and application files by monitoring, recording, and in some cases, backing up these files before they are modified. When a malware incident occurs, the system files can be returned to a previous point in time. It is possible that the previous point in time may also be a point where those files were infected with malware, so it is important to be cautious and restore to a point in time prior to the infection. Some antimalware applications are aware of these system restore points and can detect the malware, if definitions are available to do so, during the restore process. If infected files are detected, the antimalware software will attempt to modify, move, or delete them. If the files are successfully cleaned, the files will be restored. However, if a file cannot be cleaned and is deleted or quarantined, the restoration process will fail, because isolating a file results in an inconsistent restore state. If this is the case, the system will be returned to its previous state, before the restore operation began.

This process is also potentially useful because it might prevent malware from automatically restarting itself as a system service or device driver. The malware files will not be removed,

but the malware may stop automatically executing, thus giving the antimalware scanner a better chance of removing it.

### 3.4.2 Task 2: Evaluate Effectiveness

Evaluate the effectiveness of the attempts to return the system to service:

- Does it appear that malware is still on the system?
- Are any security or system settings not corrected?
- Does the system operate properly according to the user's expectations (user acceptance-type testing)?

As stated at the beginning of Task 1, restoring the system state does not remove files from a system but returns any system or application files to a previous state, potentially disabling the malware. Cleaning tools may need to be run after this step to remove the inactive malware. Evaluate whether the system meets the business risk tolerances. Go back to Step 3, if necessary.

After attempting to restore the system state and/or clean the system, if malware still appears to be on the computer, the only remaining option is to rebuild the computer (see Step 5).

## 3.5 Step 5: Rebuild the System

If it was determined in Step 2 to go directly to rebuild the system, questions were asked first to determine the risk to the data, and the data to be backed up was identified. If cleaning was attempted in Step 3 but unsuccessful, it was determined either to go to Step 4 and attempt to restore system state from backups, or to proceed to this step to rebuild the system. In this step, the system will be rebuilt from an existing image or by reinstalling the operating system.

The organisation may have decided to rebuild the system for the following reasons:

- To have the highest confidence that the system does not have any malware on it and that security or other settings have not been modified by malware.
- Because attempts to clean or restore the system have failed.
- IT has a well-documented process for rebuilding computers that is faster than cleaning or performing system restore, and there is a requirement to have the system up and running quickly.

Based on the business's priorities, the reader should decide whether to first return the system to service with basic functioning (such as business-critical applications), and then restore the user's data, settings, and appearances later, unless these are required prior to returning the system to service.

The tasks to be performed in this step are:

1. Rebuild the system.
2. Restore user settings and data.
3. Evaluate effectiveness.

Figure 5 provides a graphical representation of the tasks to be performed in this step.

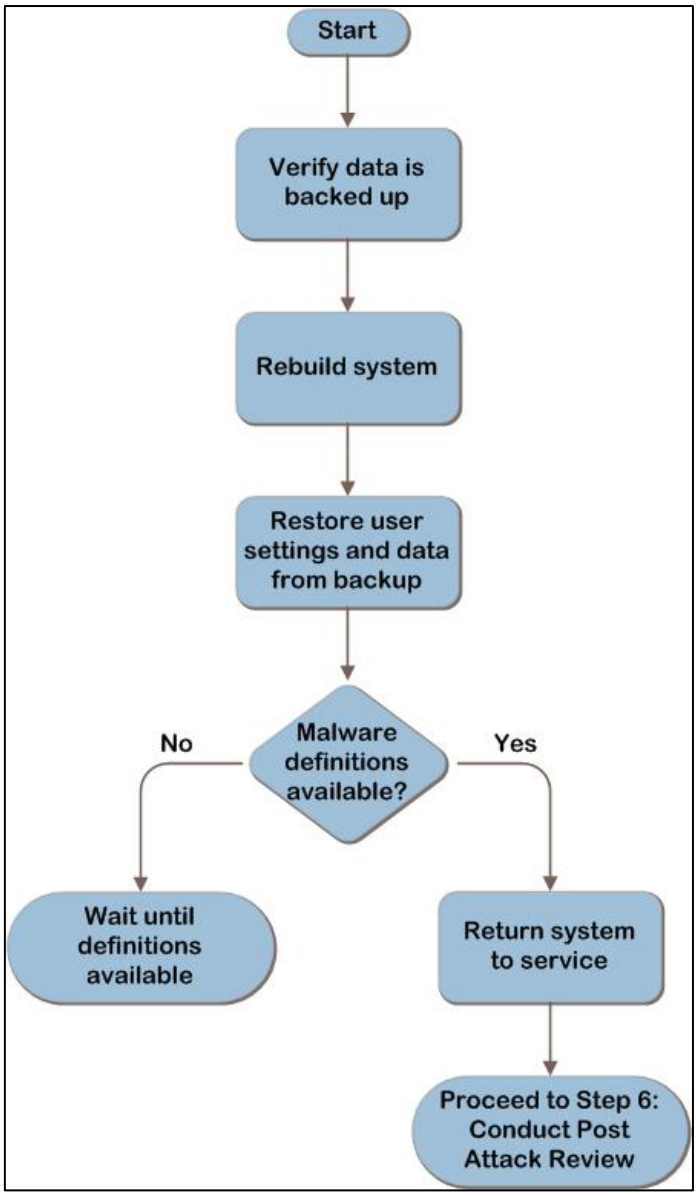


**Figure 5 Rebuild the system**

### 3.5.1 Task 1: Rebuild the System

As a reminder, any critical data that is on the system should be backed up, because rebuilding the system will destroy any data on the hard disk. See Step 2, Task 1 for more information.

After verifying the backup data for the system is trustworthy, rebuild the system. During system rebuild, the hard disk is formatted and the operating system completely reloaded, which will delete all files currently in place. If available, one could choose to rebuild the system using new or spare hard disks. Not only does this allow the original hard disks to be used for investigating the malware, it can also provide a point of return in case critical data

was missed during backup or rebuilding the system turns out to be too costly, impossible, or not necessary.

As part of the rebuild process, be sure to update the freshly installed system with the latest software updates and virus definitions, and check the system for any remaining vulnerabilities using a vulnerability scanner.

### 3.5.2 Task 2: Restore User Settings and Data

After the system is reloaded and brought up to date, the user settings and data can be restored from backup. Ensure that the files are clean prior to restoring by scanning them with a malware scanner capable of detecting the malware variant that has infected the system.

### 3.5.3 Task 3: Evaluate Effectiveness

Although rebuilding the system is the least risky option for restoring a system to a functioning state, it is still important to evaluate the effectiveness. If protection measures such as antimalware software and security updates are not put in place promptly during the rebuild process, it is possible that the machine may be reinfected. Also, restoring user data that is infected may reinfect the system.

Verify that the system is clean of malware and protected against future infections. A newly reloaded system that is found to have malware may indicate that the rebuilding process itself is contaminated.

## 3.6 Step 6: Conduct a Post-Attack Review

In the previous steps, the risk and effects of the infected system were sufficiently mitigated. This section provides suggestions for conducting a post-attack review to document the decisions made during the event to speed up the recovery process in future events. Consider the following specific actions after recovering from an incident:

- Work with legal counsel to determine whether the organisation should report the attack to the authorities if sensitive data was compromised. For example, credit card information or accidental disclosure of personally identifiable information.

- Work with legal counsel to determine whether the organisation should pursue legal steps against the attack perpetrators. In Step 2, Task 2, the decision was made about

whether to examine the malware's effects on the system. This section also provided links to information about creating a forensically sound image.

- Consider estimating how much the attack may have cost the business for internal reporting purposes. Understanding the costs of these may help IT make a business case for resources or prioritization. This may include the following elements:
    - Hours spent on the recovery
    - Cost to repair damaged equipment
    - Revenue loss
    - Cost or damage to customer and partner relations
    - Amount of lost productivity from affected workers
    - Value of any lost data

- Create or change the organisation's antimalware defense-in-depth policy.

- Recommend changes to the organisation's security policy based on the lessons learned during this incident in areas such as:
    - Default password policies.
    - Audit policies.
    - Security updates policies.
    - Firewall policies.

# 4.0 Conclusion

When it comes to responding to a malware incident, all the detection and monitoring tools available can be deployed, but still users have to be involved. Users have to be educated on how to identify infections and they need to be taught what steps to take if their system becomes infected.

# 5.0 References


- csrc.nist.gov
- http://www.techrepublic.com
- https://msdn.microsoft.com
- www.microsoft.com

# Appendix A: Malware Security Products

Microsoft offers several security products for both enterprise and home users. Table 3 provides a summary of some Microsoft malware security products.

For up-to-date information, see **www.microsoft.com/security/portal/Shared/Help.aspx#security_products**.

| **Product** | **Main segment** | | **Malicious software** | | **Spyware and potentially unwanted software** | | **Availability** |
|---|---|---|---|---|---|---|---|
| | Consumer | Business | On demand | Real-time protection | On demand | Real-time protection | |
| Microsoft Forefront Protection Suite | | X | X | X | X | X | License required |
| Forefront Endpoint Protection | | X | X | X | X | X | License required |
| Microsoft Security Essentials | X | | X | X | X | X | Free download |
| Microsoft Safety Scanner | X | | X | | X | | Free download |
| Windows Defender | X | | | | X | X | Free download |
| Microsoft Forefront Online Protection for Exchange | | X | X | X | | | Web purchase |
| Microsoft Forefront Threat Management Gateway | | X | X | X | X | X | License required |

Table 3 Summary of Malware Security Products