

Infrastructure Planning  
and Design

Malware Response

Version 1.1

Published: February 2011

Updated: November 2011

For the latest information, please see [www.microsoft.com/ipd](http://www.microsoft.com/ipd)

Copyright © 2011 Microsoft Corporation. All rights reserved. Complying with the applicable copyright laws is your responsibility.  By using or providing feedback on this documentation, you agree to the license agreement below.

If you are using this documentation solely for non-commercial purposes internally within YOUR company or organization, then this documentation is licensed to you under the Creative Commons Attribution-NonCommercial License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc/2.5/ or send a letter to Creative Commons, 543 Howard Street, 5th Floor, San Francisco, California, 94105, USA.

This documentation is provided to you for informational purposes only, and is provided to you entirely "AS IS".  Your use of the documentation cannot be understood as substituting for customized service and information that might be developed by Microsoft Corporation for a particular user based upon that user’s particular environment. To the extent permitted by law, MICROSOFT MAKES NO WARRANTY OF ANY KIND, DISCLAIMS ALL EXPRESS, IMPLIED AND STATUTORY WARRANTIES, AND ASSUMES NO LIABILITY TO YOU FOR ANY DAMAGES OF ANY TYPE IN CONNECTION WITH THESE MATERIALS OR ANY INTELLECTUAL PROPERTY IN THEM.

Microsoft may have patents, patent applications, trademarks, or other intellectual property rights covering subject matter within this documentation.  Except as provided in a separate agreement from Microsoft, your use of this document does not give you any license to these patents, trademarks or other intellectual property.

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places and events depicted herein are fictitious.

Microsoft, Active Directory, ActiveX, Bing, BitLocker, Forefront, Internet Explorer, Win32, Windows, Windows NT, Windows PowerShell, Windows Server, and Windows Vista are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries and regions.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

You have no obligation to give Microsoft any suggestions, comments or other feedback ("Feedback") relating to the documentation. However, if you do provide any Feedback to Microsoft then you provide to Microsoft, without charge, the right to use, share and commercialize your Feedback in any way and for any purpose.  You also give to third parties, without charge, any patent rights needed for their products, technologies and services to use or interface with any specific parts of a Microsoft software or service that includes the Feedback.  You will not give Feedback that is subject to a license that requires Microsoft to license its software or documentation to third parties because we include your Feedback in them.

Contents

[The Planning and Design Series Approach 1](#_Toc303850036)

[Introduction to Malware Response Guide 3](#_Toc303850037)

[Step 1: Confirm the Infection 5](#_Toc303850038)

[Step 2: Determine Course of Action 10](#_Toc303850039)

[Step 3: Attempt to Clean the System 16](#_Toc303850040)

[Step 4: Attempt to Restore System State 24](#_Toc303850041)

[Step 5: Rebuild the System 27](#_Toc303850042)

[Step 6: Conduct a Post-Attack Review 30](#_Toc303850043)

[Conclusion 31](#_Toc303850044)

[Appendix A: Malware Security Products at a Glance 32](#_Toc303850045)

[Appendix B: Examining Malware’s Effects on a System 33](#_Toc303850046)

[Appendix C: Create an Offline Scanning Kit 46](#_Toc303850047)

[Version History 58](#_Toc303850048)

[Acknowledgments 59](#_Toc303850049)

# 

# The Planning and Design Series Approach

This guide is one in a series of planning and design guides that clarify and streamline the planning and design process for Microsoft infrastructure technologies.

Each guide in the series addresses a unique infrastructure technology or scenario. These guides include the following topics:

* Defining the technical decision flow (flow chart) through the planning process.
* Describing the decisions to be made and the commonly available options to consider in making the decisions.
* Relating the decisions and options to the business in terms of cost, complexity, and other characteristics.
* Framing the decision in terms of additional questions to the business to ensure a comprehensive understanding of the appropriate business landscape.

The guides in this series are intended to complement and augment the product documentation. It is assumed that the reader has a basic understanding of the technologies discussed in these guides. It is the intent of these guides to define business requirements, then align those business requirements to product capabilities and design the appropriate infrastructure.

## Benefits of Using This Guide

Using this guide will help an organization to plan the best architecture for the business and to deliver the most cost-effective response to malicious software (also called malware).

Benefits for Business Stakeholders/Decision Makers:

* Most cost-effective design solution for an implementation. Infrastructure Planning and Design (IPD) eliminates over-architecting and overspending by precisely matching the technology solution to the business needs.
* Alignment between the business and IT from the beginning of the design process to the end.

Benefits for Infrastructure Stakeholders/Decision Makers:

* Authoritative guidance. Microsoft is the best source for guidance about the design of Microsoft products.
* Business validation questions to ensure the solution meets the requirements of both business and infrastructure stakeholders.
* High-integrity design criteria that includes product limitations.
* Fault-tolerant infrastructure, where necessary.
* Proportionate system and network availability to meet business requirements.
* Infrastructure that is sized appropriately to meet business requirements.

**Benefits for** Consultants or Partners:

* Rapid readiness for consulting engagements.
* Planning and design template to standardize design and peer reviews.
* A “leave-behind” for pre- and post-sales visits to customer sites.
* General classroom instruction/preparation.

Benefits for the Entire Organization:

Using this guide should result in a design that will be sized, configured, and appropriately placed to deliver a solution for achieving stated business requirements, while considering the performance, capacity, manageability, and fault tolerance of the system.

# Introduction to Malware Response Guide

The goal of this malware response guide 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.

When a malware attack occurs, a number of factors—some conflicting—must be considered quickly and simultaneously to restore service to the system. Understanding how the system was compromised while simultaneously returning the system to operation as quickly as possible is a common conflicting issue that this guide addresses. This guide does not resolve this conflict: The reader must do so based on the priorities of the business.

When deciding which course of action to take to control the attack and quickly restore the system, consider the following:

* 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 organization.
* 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 organization is willing to accept when responding to and recovering from a malware attack.

## Assumptions

To limit the scope of material in this guide, the following assumptions have been made:

* The reader has basic knowledge of malware. This guide does not attempt to educate the reader on malware types, propagations, or specific variants. To learn more about malware, visit the Microsoft Malware Protection Center at [www.microsoft.com/security/portal](http://www.microsoft.com/security/portal) or see the Wikipedia article on malware at <http://en.wikipedia.org/wiki/Malware>.
* The reader is familiar with the organization’s incident management procedures, should they exist.
* Some of the tasks in this guide may require information technology (IT) expertise or administrative rights. Thus, it may not be appropriate for users to perform them.

## Malware Response Design Process

This guide describes decisions and activities to perform when responding to and recovering from a malware incident.

The decisions and activities to perform in this 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.

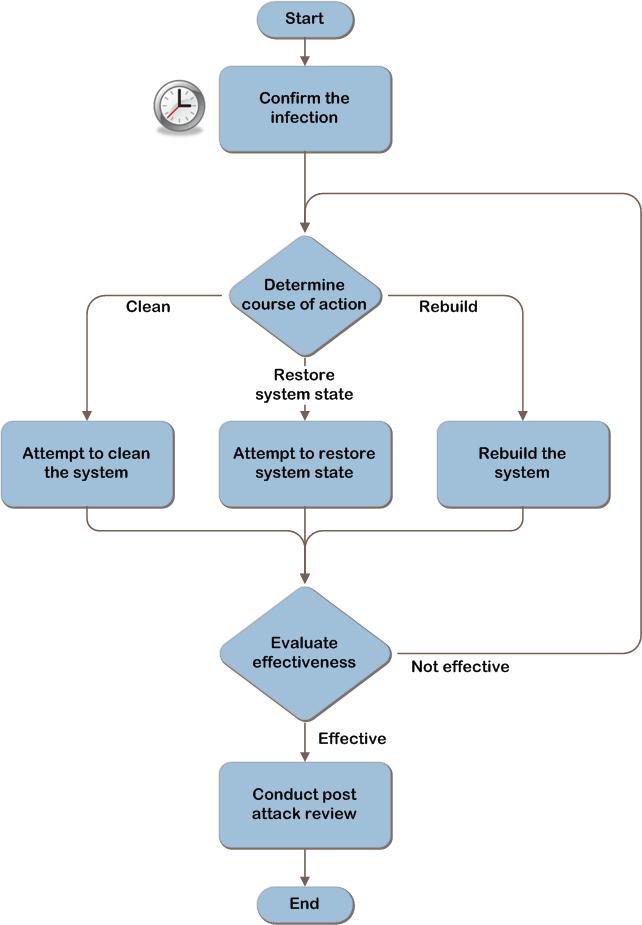


Figure 1. Response to a malware incident at a high level

# Step 1: Confirm the Infection

This step begins when an organization 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.

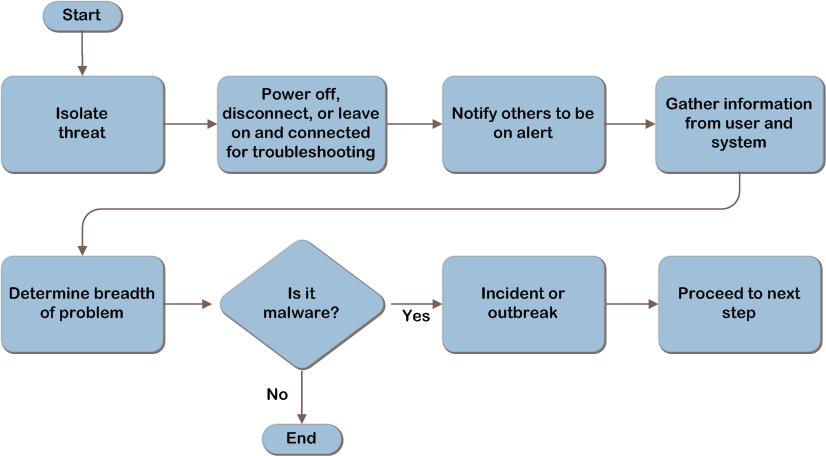


Figure 2. Confirm the infection

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 organization to begin rebuilding machines in a quarantined network away from potential infection until detection and prevention methods are present.

## 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 organization. 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 organization’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.

## 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.

## Validating with the Business

To help understand the organization’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.

## Task 3: Gather Information About the Threat

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

### 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 this is not a complete list, these are 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.

### 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 or Microsoft® System Center Configuration Manager:

**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.

## 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.

## Task 5: Determine Whether Malware Is Present

Evaluate the evidence to determine whether the organization 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 the Microsoft Malware Protection Center at [www.microsoft.com/security/portal](http://www.microsoft.com/security/portal) or other 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 organization’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.

## Step Summary

In this step, actions to immediately contain an infection were described. Information was gathered from the user and about the system to help assess the breadth of the problem. After completing this step, examine the data gathered. If there is evidence that a malware incident or outbreak is occurring, continue to Step 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 organization.

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 optimize 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 organization 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 organization. As an example, if thousands of computers in the organization are infected but the malware is well documented, the business may choose to trigger a scan and clean from a central administrative console. This should be the only action if the business has high confidence the system will be clean and will not be infected with any other malware. However, if the payload is unknown, and because manually cleaning the malware does not guarantee that no secondary infections will occur, the business may choose to take the slower but less risky route of rebuilding the machine by reinstalling the operating system and applications.

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.

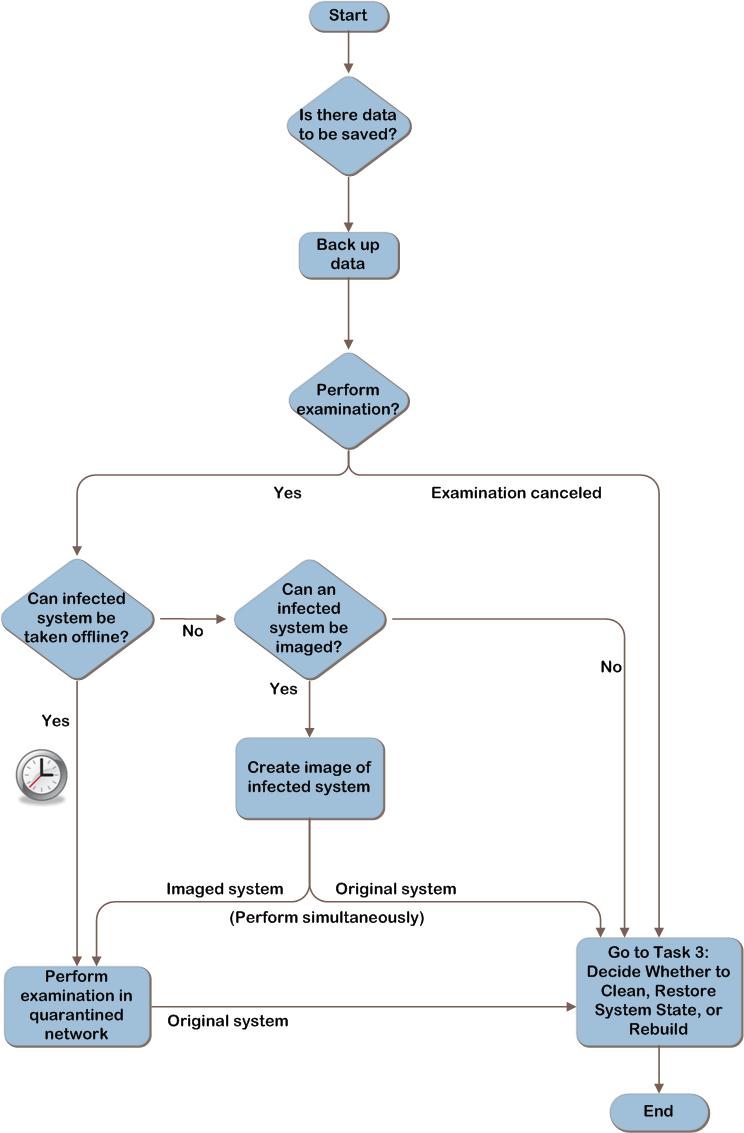


Figure 3. Determine the course of action

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.

## 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 categorized 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.

### 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 (such as booting in to a Windows® Preinstallation Environment [Windows PE] or attaching the drive as a subordinate drive in another, noninfected system) 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.

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

Decide whether the organization wants the malware’s effects on the system examined. Examination can be beneficial to the organization 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 organization may decide that it is not important to know the details about the malware infection.

The primary factors when considering examination are whether the organization 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.

Note   If the organization believes that legal action is a possible outcome from this incident, then special steps should be taken to ensure the image is legally acceptable. This is outside the scope of this guide. See “Fundamental Computer Investigation Guide for Windows” at <http://technet.microsoft.com/en-us/library/cc162846.aspx> and “Computer Forensics: Disk Imaging Overview” at <http://technet.microsoft.com/en-us/library/cc512667.aspx> for more information relative to creating a forensically sound image of the system.

If it is determined that there is sufficient time to examine the effects of the malware on an infected system or to image the system, refer to Appendix B: “Examining Malware’s Effects on a System” for more information about performing the examination. 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’s 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.

## 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 organization’s level of confidence that the option selected will reduce the malware risk to a level the organization 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 organization 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 organization 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 organization, 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.

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

| **Method** | **Pros** | **Cons** |
| --- | --- | --- |
| Clean | * Generally simple and fast process, if cleaning tools are available. * Best chance of keeping the applications and data intact. * 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. * Removes malware but does not restore system settings and files. * 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. * Less destructive than rebuilding the system. * Generally fast process. | * Does not necessarily remove malware—may only inactivate it. * 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. * 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. |

Note   If the decision is made to clean an infected system, the organization’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.

## 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.

## Step Summary

In this step, the risk to data was determined. If backups were required, they were performed before proceeding with the chosen course of action. A decision was made whether to examine the malware’s effects on the system. Also, it was decided whether to clean the malware, restore system state, or rebuild the system.

# 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.

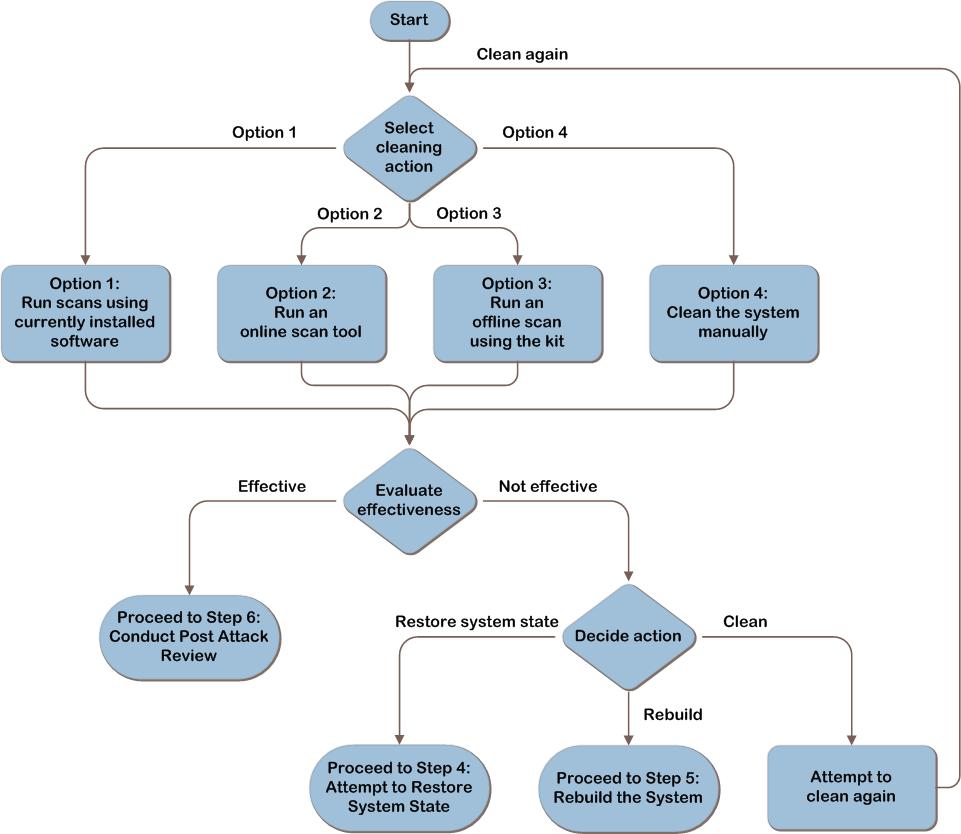


Figure 4. Attempt to clean the system

## 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 organization 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 organization’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.

See the following websites for more information about how to start computers running Windows operating systems in safe mode:

* Windows 7. See “Start your computer in safe mode” at <http://windows.microsoft.com/en-US/windows7/Start-your-computer-in-safe-mode>.
* Windows Vista®. See “Advanced startup options (including safe mode)” at <http://go.microsoft.com/fwlink/?LinkId=87010>.
* Windows XP. See the Microsoft Support article “A description of the Safe Mode Boot options in Windows XP” at <http://support.microsoft.com/kb/315222>.

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 organization 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. For example, scanning tools such as RootkitRevealer at <http://technet.microsoft.com/en-us/sysinternals/bb897445.aspx> are designed to examine the behavior of the infected computer while it’s online. This type of tool is not effective when performing offline scanning. Using a combination of methods and/or antimalware products may be used to further mitigate the risk.

### 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 organization 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.

### 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. For more information, see the Microsoft Support article, “How do I reset the hosts file back to the default?” at <http://support.microsoft.com/kb/972034>. If the actions described in that article do not solve the problem, then Option 3 or Option 4 may be needed.

The “Additional Reading” section in this step provides links to online scan software.

### 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. Appendix C: “Create an Offline Scanning Kit” provides instructions about how to do this.

A disk cannot be scanned for malware if it has been encrypted with a tool such as BitLocker® Drive Encryption 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.

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

Note   Because many malware attacks are released in variants, such as MyDoom@A, MyDoom@B, and so on, it is important to use cleaning procedures or tools to clean the specific version of the malware from the system.

The Microsoft Safety Scanner at [www.microsoft.com/security/scanner/en-us/default.aspx](http://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.

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

Table 2. Pros and Cons of System Cleaning Methods

| **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. * Faster than other methods, because it uses already-installed software. | * Some remediation tasks may require administrative privileges. * Definitions must be updated to include detection for the malware (assuming that original real-time protection did not detect the malware). * 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. * Requires starting the computer into its installed operating system, which could allow malware to continue its course. * Cannot be triggered to run automatically across a number of computers. * Does not provide real-time protection. |
| 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. * An offline scanning kit must be created. * 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. * Some antimalware vendors release specialized cleaning tools. | * Requires starting the computer into its installed operating system, which could allow malware to continue its course. * Not all malware is well documented. * Can be complex to perform. Requires a detailed understanding of how Windows operating systems work and significant expertise with malware. |

## 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’s 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 organization 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 organization 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).

## Step Summary

In this step, the system cleaning plan was put into effect. Attempts were made to remove the malware using automated tools such as antimalware products. An alternative to cleaning the system was also presented: rebuilding the system from installation media that is known to be trustworthy. This is the only approach that guarantees the elimination of malware from the file system. However, the cost can be high if procedures to facilitate system recovery, such as automatic backup and automated deployment tools, were not already in place.

## Additional Considerations

Windows Defender helps provide protection against spyware. It is included with the operating system for Windows 7 and Windows Vista and is free to download for computers running Windows XP. To download Windows Defender or get more information on running scans, go to [www.microsoft.com/windows/products/winfamily/defender/support.mspx](http://www.microsoft.com/windows/products/winfamily/defender/support.mspx).

Microsoft Security Essentials is a consumer-oriented offering that helps provide protection against spyware, viruses, and other malicious software. It is a separate download for computers running Windows XP (with Service Pack 2 [SP2] or SP3), Windows Vista, and Windows 7. To download Microsoft Security Essentials and get more information relative to running scans, go to [www.microsoft.com/security\_essentials](http://www.microsoft.com/security_essentials).

The Microsoft Safety Scanner at [www.microsoft.com/security/scanner/en-us/default.aspx](http://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.

For enterprise customers, Microsoft Forefront® Endpoint Protection helps provide unified protection from viruses, spyware, and other current and emerging threats for business client computer, portable computer, and server operating systems. See [www.microsoft.com/forefront/clientsecurity](http://www.microsoft.com/forefront/clientsecurity) for more information.

## Additional Reading

* Microsoft Malware Protection Center: [www.microsoft.com/security/portal/Threat/Threats.aspx](http://www.microsoft.com/security/portal/Threat/Threats.aspx)
* Windows Defender: [www.microsoft.com/windows/products/winfamily/defender/default.mspx](http://www.microsoft.com/windows/products/winfamily/defender/default.mspx)
* Windows Defender Technical Overview: <http://technet2.microsoft.com/WindowsVista/en/library/94d9603c-91ef-4a7a-8811-4904a1fb540c1033.mspx?mfr=true>.
* Forefront Endpoint Protection: [www.microsoft.com/forefront/endpoint-protection/en/us/default.aspx](http://www.microsoft.com/forefront/endpoint-protection/en/us/default.aspx)
* For Windows 7: “Start your computer in safe mode”: <http://windows.microsoft.com/en-US/windows7/Start-your-computer-in-safe-mode>
* For Windows Vista: “Advanced startup options (including safe mode)”: <http://windows.microsoft.com/en-US/windows-vista/Advanced-startup-options-including-safe-mode>
* Microsoft Support article “A description of the Safe Mode Boot options in Windows XP”: <http://support.microsoft.com/kb/315222>
* Sysinternals tools: <http://technet.microsoft.com/sysinternals>
* Microsoft Safety Scanner: [www.microsoft.com/security/scanner/en-us/default.aspx](http://www.microsoft.com/security/scanner/en-us/default.aspx)
* Creating a Strong Password Policy: <http://technet.microsoft.com/en-us/library/cc736605(WS.10).aspx>
* “List of antivirus software vendors”: <http://support.microsoft.com/kb/49500>
* Kaspersky Online Virus Scanner: <http://usa.kaspersky.com/downloads/free-virus-scanner.php>
* Symantec Security Check: <http://security.norton.com/sscv6/default.asp?langid=ie&venid=sym>
* Panda ActiveScan 2.0: [www.pandasecurity.com/activescan](http://www.pandasecurity.com/activescan)
* Trend Micro HouseCall: <http://housecall.trendmicro.com/>
* AVG Anti-Virus Free Edition 2012: [www.avg.com/us-en/free-antivirus](http://www.avg.com/us-en/free-antivirus)
* “How do I remove a computer virus?”: <http://windows.microsoft.com/en-us/Windows7/How-do-I-remove-a-computer-virus>

# 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.

## 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.

The following paragraphs describe tools that can be used to restore the system state.

* System Restore. Applies to Windows 7, Windows Vista, and Windows XP. System Restore uses a feature called system protection to regularly create and save restore points on the computer. These restore points contain information about files, registry settings, and other system information that Windows uses. Restore points can also be created manually. Unlike **Last Known Good Configuration** (described below), changes made with System Restore can be undone (unless made in safe mode), and different points in time to which the system can be restored may be available.
* Windows Recovery Environment. For computers running Windows 7, Windows Vista, Windows Server 2008, and Windows Server 2008 R2, the Windows Recovery Environment (Windows RE) is launched automatically when a computer fails to start or manually from many media, including hard disks, USB drives, optical media (such as an operating system installation disc) and the Pre-Boot Execution Environment (PXE). The Startup Repair tool in Windows RE automates the diagnosis and repair of an operating system that cannot be restarted. It can also be used as a starting point for various tools for manual system recovery, including Windows System Restore (if available for that operating system), or to restore a Windows Backup system image.
* Last Known Good Configuration. Applies to Windows 7, Windows Vista, Windows XP, Windows Server 2003, and Windows Server 2008. **Last Known Good Configuration** is a snapshot of the last time (and only the last time) that the computer started successfully. This feature is similar to System Restore but affects the system configuration and driver settings, while System Restore monitors all system folders, including the desktop. If the organization does not know with certainty that the last time the system started was prior to the malware infection, then this is not a viable option.
* Automated System Recovery (ASR).For computers running Windows XP or Windows Server 2003, ASR provides a simple means to quickly back up both the boot volumes and system volumes on the computer, which will provide the ability to more rapidly restore the system in the event of an infection or failure. ASR is useful, because it can restore the entire computer, including user data and applications; however, ASR backups have to be created prior to malware infection.
* Windows Backup. Windows Backup is useful, because it can restore the entire computer, including user data and applications; however, backups have to be created prior to malware infection to perform a restore. Differences between versions of Windows Backup are in the degree of automation and the flexibility of specifying whether to back up only certain files or directories and/or system settings. Windows Backup for Windows XP is the least automated version; however, it is flexible. Windows Backup for Windows Vista is highly automated, but it is not as flexible as Windows Backup for Windows XP. Windows Backup for Windows 7 is both highly automated and more flexible than the version for Windows Vista. Some malware may interfere with the Windows Backup process, because the restore task is run from the infected operating system.

## 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).

## Step Summary

In this step, an attempt was made to restore the system state, and the restored system was evaluated for the effectiveness of malware removal.

## Additional Reading

* Microsoft Support article, “How to restore Windows XP to a previous state”: <http://support.microsoft.com/kb/306084>.
* Windows 7 Features: Backup and Restore: <http://windows.microsoft.com/en-US/windows7/products/features/backup-and-restore>.
* Microsoft Support article, “How antivirus software and System Restore work together”: <http://support.microsoft.com/?kbid=831829>.
* Automated System Recovery (ASR) overview: <http://technet.microsoft.com/en-us/library/cc779908(WS.10).aspx>.
* Microsoft Support article, “Automated System Recovery overview in Windows XP”: <http://support.microsoft.com/kb/818903>.
* A Guide to Windows Vista Backup Technologies: <http://technet.microsoft.com/en-us/magazine/2007.09.backup.aspx>
* Backing Up and Restoring Data (Windows XP Professional Resource Kit): <http://technet.microsoft.com/en-us/library/bb457113.aspx>
* Checklist: Recover Files, Folders, Applications, Volumes, or the Operating System: <http://technet.microsoft.com/en-us/library/cc732571.aspx>.
* Windows Recovery Environment Technical Reference: <http://technet.microsoft.com/en-us/library/dd744255.aspx>.

# 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 organization 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.

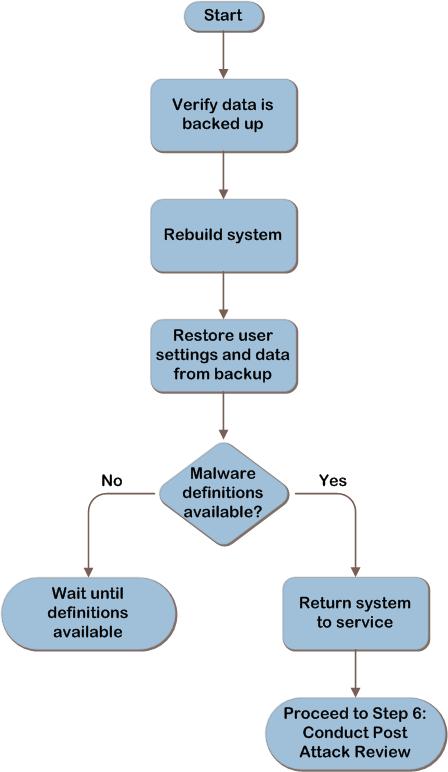


Figure 5. Rebuild the system

## 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.

The actual process of rebuilding the system is outside the scope of this document. For more information relative to deployment choices, see “Choosing a Deployment Strategy” at <http://technet.microsoft.com/en-us/library/dd919185(WS.10).aspx>. The Microsoft Deployment Toolkit (MDT) is a free Solution Accelerator that supports deployment of Windows 7, Microsoft Office 2010, and Windows Server 2008 R2 in addition to deployment of Windows Vista, Windows Server 2008, Windows Server 2003, and Windows XP. See the MDT site at [www.microsoft.com/mdt](http://www.microsoft.com/mdt) for more information.

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 such as the Microsoft Baseline Security Analyzer (MBSA), which is available for download at <http://technet.microsoft.com/en-us/security/cc184924.aspx>. Microsoft Security Compliance Manager (SCM) provides centralized security baseline management features, a baseline portfolio, customization capabilities, and security baseline export flexibility to accelerate the organization’s ability to efficiently manage the security and compliance process for the most widely used Microsoft technologies. See the SCM site at [www.microsoft.com/scm](http://www.microsoft.com/scm) for more information.

## 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. The SCM tool at [www.microsoft.com/scm](http://www.microsoft.com/scm) can be used to reset security settings on the system to a baseline.

## 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.

## Step Summary

In this step, the system was rebuilt either from image or by reinstalling the operating system. The user settings and data were restored, and then the activities performed were evaluated for effectiveness.

## Additional Reading

* Microsoft Security Bulletin Search: [www.microsoft.com/technet/security/current.aspx](http://www.microsoft.com/technet/security/current.aspx)
* Microsoft Baseline Security Analyzer: <http://technet.microsoft.com/en-us/security/cc184924.aspx>

# 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 organization 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 organization 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 organization’s antimalware defense-in-depth policy.
* Recommend changes to the organization’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.

## Step Summary

This step described post-attack items to consider for lessons learned.

## Additional Reading

* Make an Incident Response Plan: [www.windowsecurity.com/articles/Make\_an\_Incident\_Response\_Plan.html](http://www.windowsecurity.com/articles/Make_an_Incident_Response_Plan.html)
* Creating a Computer Security Incident Response Team: A Process for Getting Started: [www.cert.org/csirts/Creating-A-CSIRT.html](http://www.cert.org/csirts/Creating-A-CSIRT.html)
* Microsoft Malware Protection Center: [www.microsoft.com/security/portal](http://www.microsoft.com/security/portal)
* Microsoft Security Intelligence Report: [www.microsoft.com/security/portal/Threat/SIR.aspx](http://www.microsoft.com/security/portal/Threat/SIR.aspx)

# Conclusion

This guide provided recommendations for limiting the risk of malware infecting computers in organizations. It introduced a defense-in-depth approach to protecting systems against viruses, spyware, and other types of undesirable software. It also described approaches to investigating outbreaks and cleaning infected systems. Appendix C presents three approaches to building a bootable CD-ROM or DVD that the organization can use to scan and clean systems while they are offline.

Because of the changing nature of malware, no single antimalware or antispyware solution can guarantee protection against all attacks. If, after following the steps in this guide, more help is needed with malware-related issues, contact Microsoft Product Support Services:

 For support within the United States and Canada, call toll-free 866-727-2338 or  
866-PCSAFETY.

 For support outside the United States and Canada, visit the Malware Protection Center website at [www.microsoft.com/security/portal](https://www.microsoft.com/security/portal) and the Learn more about malware: Guidance and advice website at [www.microsoft.com/security/portal/Shared/Help.aspx](https://www.microsoft.com/security/portal/Shared/Help.aspx).

## Additional Reading

* The Microsoft Malware Protection Center, which provides the latest information on major desktop and email threats to computers running Windows: [www.microsoft.com/security/portal](http://www.microsoft.com/security/portal)
* The Microsoft Security Response Center, which responds to vulnerabilities in Microsoft products: [www.microsoft.com/security/msrc/default.aspx](http://www.microsoft.com/security/msrc/default.aspx)
* The Microsoft Security Response Alliance, which provides information about the Microsoft Virus Initiative, the Virus Information Alliance, and other member organizations: [www.microsoft.com/security/msra/default.mspx](http://www.microsoft.com/security/msra/default.mspx)
* The Trustworthy Computing Security Development Lifecycle, which provides methodology to increase software security: <http://msdn.microsoft.com/en-us/library/ms995349.aspx>
* Microsoft Safety Scanner: [www.microsoft.com/security/scanner/en-us/default.aspx](http://www.microsoft.com/security/scanner/en-us/default.aspx)
* Microsoft Security Essentials: [www.microsoft.com/security\_essentials/](http://www.microsoft.com/security_essentials/)
* Windows Defender: [www.microsoft.com/defender](http://www.microsoft.com/defender)
* Microsoft Forefront: [www.microsoft.com/forefront/](http://www.microsoft.com/forefront/)
* Microsoft Security TechCenter: [www.microsoft.com/technet/security/default.mspx](http://www.microsoft.com/technet/security/default.mspx)
* Microsoft Safety & Security Center: [www.microsoft.com/protect/default.aspx](http://www.microsoft.com/protect/default.aspx)
* Trustworthy Computing: [www.microsoft.com/about/twc/en/us/default.aspx](http://www.microsoft.com/about/twc/en/us/default.aspx)
* For information about an alliance dedicated to eliminating spam and working with law enforcement officials and Internet service providers to prosecute spam operations, see “America Online, Microsoft and Yahoo! Join Forces Against Spam”: [www.microsoft.com/presspass/press/2003/apr03/04-28JoinForcesAntispamPR.mspx](http://www.microsoft.com/presspass/press/2003/apr03/04-28JoinForcesAntispamPR.mspx)
* National Institute of Standards and Technology (NIST) Special Publication 800-61 Revision 1 Computer Security Incident Handling Guide: <http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf>

# Appendix A: Malware Security Products at a Glance

Microsoft offers several security products for both enterprise and home users. Table A-1 provides a summary of all Microsoft malware security products as of this guide’s publishing. For up-to-date information, see [www.microsoft.com/security/portal/Shared/Help.aspx#security\_products](http://www.microsoft.com/security/portal/Shared/Help.aspx#security_products).

Table A-1. Summary of Malware 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 needed |
| Forefront Endpoint Protection |  | X | X | X | X | X | License needed |
| Microsoft Security Essentials | X |  | X | X | X | X | Free via web download |
| Microsoft Safety Scanner | X |  | X |  | X |  | Free via web download |
| Windows Defender | X |  |  |  | X | X | Free via Download Center |
| Microsoft Forefront Online Protection for Exchange |  | X | X | X |  |  | Web purchase |
| Microsoft Forefront Threat Management Gateway |  | X | X | X | X | X | License needed |

# 

# Appendix B: Examining Malware’s Effects on a System

This appendix provides information on conducting a basic examination of malware’s effects on a system. It is optional, as the business may have decided that because of time constraints or lack of expertise, it is not in a position to conduct an examination of the outbreak. In addition, this topic is large, and because every malware outbreak is different, it is not possible to cover every situation comprehensively in this guide.

Note   If the organization thinks legal action is a possible outcome of this incident, then expertise in IT forensics is a requirement. This is outside the scope of this guide. See the *Fundamental Computer Investigation Guide for Windows* at <http://technet.microsoft.com/en-us/library/cc162846.aspx> and Computer Forensics: Disk Imaging Overview at <http://technet.microsoft.com/en-us/library/cc512667.aspx> for more information on creating a forensically sound image of the system.

Ideally, the examination of the malware will be performed by a member of the security team with a dedicated set of applications and utilities to gather the required information with as much automation as possible.

The tasks to be performed in this step are:

1. Gather the basic information.
2. Gather the details.
3. Examine the operating system elements.
4. Evaluate the data.
5. Determine whether the issue is real.

## Task 1: Gather the Basic Information

Gather the basic information in this task. The following questions can be used as a starting point for this process; they should be modified to meet the requirements of the organization.

* **What is the operating system and what security updates have been applied?** This may help rule out some malware possibilities.
* **Is the user logged on with an account that has administrator privileges?** If so, the system is more likely to have been compromised and to a greater extent than if the user was logged in with a restricted account.
* **Is the user using a strong password or passphrase?** A weak password increases the likelihood that an attacker compromised the system by guessing the user’s password.
* **Has this system suffered a malware attack before?**

This last question is important, as previous attacks often create vulnerabilities that can lead to subsequent attacks unless they are fixed. If the answer to this question is “Yes,” ask the following questions:

* When did the previous attack occur?
* Who handled the case and what was the case number?
* Is there any information about what was done at that time?

## Task 2: Gather the Details

In this task, more details are gathered. At this point, it may be possible to determine whether a new malware attack is the cause of the problem. If not, a higher level of technical information may be required and a support technician may need to physically visit (or, if possible, gain remote control to) the suspect system. The following questions can be used to gather more detailed information and determine whether the system has been attacked by a hacker or malicious code.

* Does the device have a firewall enabled on it or in front of it? If so, what ports are open to the Internet?
* Are applications crashing? If so, contact the application vendors immediately to determine the root cause. For example, current Microsoft applications provide error reporting tools that can be used to send in a crash report.
* Have any security updates for this system been released but not installed?
* What kind of password policy does the system have? What is the minimum password length? What are the password complexity requirements?
* Are there any network connections reported by the Netstat utility to external IP addresses or suspicious IP addresses?

## Task 3: Examine the Operating System Elements

In this task, an attempt is made to determine which operating system files were introduced or modified by the attack. As part of this examination, look for changes in the following areas:

* Active processes and services
* Startup folders
* Scheduled applications
* The local registry
* Files
* Users and groups
* Shared folders (including hidden folders)
* Opened network ports
* System event logs

Techniques that can be used for checking these operating system elements are explained in the following sections.

### Active Processes and Services

Infected systems are likely to have had new processes introduced into their memory. Using specialized process-listing tools such as PsTools and the Process Explorer freeware program is recommended to provide a more user-friendly interface. These tools are available from the Sysinternals website at <http://technet.microsoft.com/sysinternals>. They make it possible to see not only the path to the image file, but also the process tree.

To help minimize the number of entries in the process list and therefore help in the identification of any rogue processes, close all valid applications and any valid background applications, such as instant messenger windows, email monitors, or non-Microsoft utilities that stay resident in memory.

If a specialized tool is not available, the Windows Task Manager tool in all Windows systems can be used as a quick check for active processes running on the system. However, because Task Manager does not show the path to the image that launched the process, it is impossible to determine whether a malware attack launched as “svrhost” or “svchost” is a legitimate process.

Complete the following steps to examine the active processes using Task Manager:

**To examine active processes on a computer running Windows**

1. Press Ctrl+Alt+Delete simultaneously to bring up the Windows Security window, and click Start Task Manager.
2. Click the Processes tab.
3. Resize the Windows Task Manager window to display as many of the active processes as possible.
4. Select the View option from the menu bar, and then click Select Columns.
5. Select the following columns:

* PID (Process Identifier)
* CPU Usage
* CPU Time
* Memory Usage
* Peak Memory Usage
* I/O Reads
* I/O Writes

1. Click OK and resize the window to show as many of these columns as possible.

The order of the columns can be sorted by clicking any column title. Use this sorting method for each of the listed columns, and determine which processes are using which resources.

Note   To obtain a printout of this list for future reference, make Process Explorer or the Windows Task Manager the active window, and then press ALT+PRT SCRN. A screen shot of the list will be created in the computer’s clipboard, which can be pasted into the Microsoft Paint application or Microsoft Word and printed.

Use the following tips to check processes on a computer suspected of running malware:

* Check for any instances of running Telnet or File Transfer Protocol (FTP) services.
* If a process is not clear, use an Internet search engine such as Microsoft Bing® to try to find some information about it.
* Check the path to the image file for a recognizable image for that process.
* Look for both running and stopped services.

Examples of possibly suspicious processes include:

* ServuFTP
* Ocxdll.exe
* Kill.exe
* Mdm.exe
* Mdm.scr
* Mt.exe
* Ncp.exe
* Psexec.exe
* Win32load.exe

Note   This list is provided to illustrate examples of the type of file names that have been used in the past. Most attacks will use a different name, so it is important to be able to spot the unusual entries in the task list and understand the naming techniques used by malware writers.

### Startup Folders

It is possible that the malware has attempted to launch itself by modifying the startup folders of the system.

Note   The precise path for these folders will change depending on the operating system being examined. The following information is for operating systems running Windows 7 and Windows Vista.

Two areas of the startup folder should be checked. The first is the Startup folder, which can be found at the following default location on computers running Windows 7:

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup

The second is the user profile path for the currently logged-on account, although it is important to check all profiles that have been created on the system and not just the account that is currently logged on. This information will be found at:

C:\Documents and Settings\User\_Name\Start Menu, where User\_Name is the logon ID of the defined user on the system being inspected.

Check each of the entries in each startup folder to ensure no malware is attempting to start during a system startup. Microsoft recommends using the Autoruns for Windows utility to provide a more user-friendly interface. This tool is available from the Sysinternals website at <http://technet.microsoft.com/sysinternals>. It makes it possible to easily see what programs are configured to run during system startup or login and shows the entries in the order Windows processes them. It includes the startup folder, Run, RunOnce, and other registry keys and can be configured to show other locations, including Windows Explorer shell extensions, toolbars, browser helper objects, Winlogon notifications, auto-start services, and much more.

### Scheduled Applications

Malware also may try to use the Windows Scheduler service to launch an unauthorized application. To confirm that this is not the case, the scheduler queue should be checked.

**To check the scheduler queue**

1. Click Start, and then click Run. In the Run box, type cmd to open a Command Prompt window.
2. At the command prompt, type at and then press Enter.
3. If any entries appear in the list, check for unauthorized or suspicious applications, and create a report for future examination using the following command:

at >C:\AT\_Queue\_Report.txt

Executing this command creates a text file in the root of drive C. Move this file to a removable disk for future examination. Review the text file to determine whether any unauthorized applications are scheduled in the queue.

Once the active and scheduled processes have been examined, it may be possible to identify the processes that the attack introduced. After these have been documented, restart the system and repeat the examination to determine whether the attack compromised other areas of the system and allowed the rogue processes to be launched at startup. If so, examine the system's boot files and registry to find the mechanism used to maintain the rogue processes.

Windows Sysinternals utilities, such as Autoruns, provide another way to list start locations. For more information, see the Sysinternals Utilities Index page at <http://technet.microsoft.com/en-us/sysinternals/bb545027.aspx>.

### The Local Registry

Because the completed system registry is a large and complex data store, it may be beneficial to create a copy of the entire system registry for a detailed examination after completing the attack recovery process.

The Backup utility that is included with all versions of Windows can be used to back up and restore the entire registry. If Backup is already used to regularly back up the hard disk, the registry can easily be used in these backups. To back up the registry with the Backup application, select System State in addition to the desired drives, files, and folders to include in the backup set.

Because the system state includes other system-specific information as well as the registry, these backup files can be hundreds of megabytes in size. Another option is to use the registry editor utilities that also come with all versions of Windows. These utilities are ideally suited to make copies of the registry. Windows XP and Windows Server 2003 have two registry editor tools, Regedit and the command-line tool Reg.exe.

**To make a backup copy of the registry using Regedit**

1. Click Start, and then click Run. In the Run box, type regedit, and then press Enter.
2. In the left pane, select **My Computer**. Then, from the File menu, click Export.
3. In the File name box, type a name and location for the copy of the registry file.
4. Under Export range, click All, and then click Save.

Detailed information about how to use Regedit and Reg.exe can be found in the “Windows Server 2003 Resource Kit Registry Reference” section of the Windows Server 2003 Deployment Guide at <http://technet.microsoft.com/en-us/library/cc778196(WS.10).aspx>.

Important   Because this disk will be exposed to the malware, ensure that it is not exposed to other systems until an effective method of control has been established.

Once a successful registry backup has been completed, check the following areas for any unusual file references:

* HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\SessionManager\KnownDLLs
* HKEY\_LOCAL\_MACHINE\System\ControlSet001\Control\Session Manager\KnownDLLs
* HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\Current Version\Run
* HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\Current Version\RunOnce
* HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\Current Version\RunOnceEx
* HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices
* HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Windows ("run=" line)
* HKEY\_CURRENT\_USER\Software\Microsoft\Windows\Current Version\Run
* HKEY\_CURRENT\_USER\Software\Microsoft\Windows\Current Version\RunOnce
* HKEY\_CURRENT\_USER\Software\Microsoft\Windows\Current Version\RunOnceEx
* HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\RunServices
* HKEY\_CURRENT\_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows ("run=" value)

These areas of the Registry are often targeted by malicious code because they allow the malware to launch itself at system startup. For example, the W32@.Mydoom.G@mm worm added the following value:

"(Default)" = "%System%\<random\_filename>"

to the following registry keys:

* HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run
* HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

Another area that has been targeted is the following key:

HKEY\_CLASSES\_ROOT\CLSID\{E6FB5E20-DE35-11CF-9C87-00AA005127ED}\InProcServer32

This key controls the DLL files that Windows Internet Explorer® (Explorer.exe) loads. For example, the Mydoom worm and its variants add an entry here to load a DLL file that causes a vulnerability and allows a backdoor attack.

The W32.Netsky.D@mm worm deletes this key and the following keys altogether:

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\PINF

HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\WksPatch

Another tool that can be extremely useful for examining Windows XP– and Windows Server 2003–based systems is the System Configuration Utility. It is possible to view and modify a variety of startup and configuration information as well as review the current services list using this tool. More information on using this tool can be found in the Windows XP Professional Resource Kit. This information is also available online on the System Configuration Utility page at <http://support.microsoft.com/kb/310560>. The System Configuration Utility is included with later versions of Windows. To launch it, do the following:

Click Start, and then click Run. In the Run box, type msconfig, and then press Enter.

Note   To use System Configuration Utility, the person performing this operation must be logged on as an administrator or a member of the Administrators group.

### Files

Most malware will modify one or more files on a computer's hard disk, and finding which files have been affected may be a difficult process. Look for newly created files with normal-looking file names but in unusual locations. If the system was created from an image, the infected system may be compared directly with a fresh system created from this image.

If this option is not available, another method to determine which files have been changed is to use a system-wide search of all files that have changed since the malware was first introduced to the system. This can be achieved using the Windows Search tool. Figure B-1 shows how to narrow the search for infected files using the Date modified option.

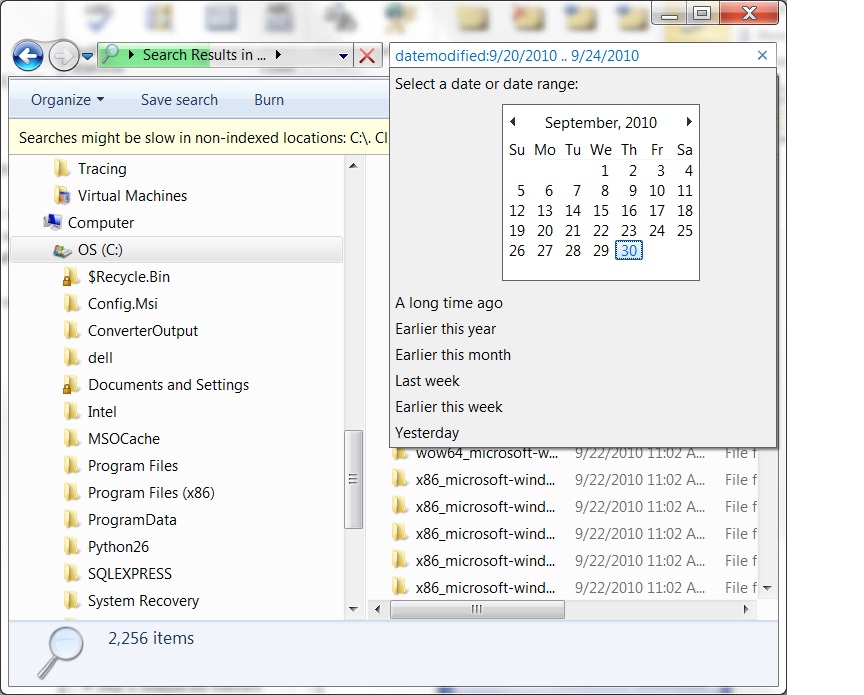


Figure B-1. The Search Results advanced options dialog box

With the options set as in Figure B-1, all files that were created when the malware was introduced onto the host (in this example, September 20, 2010, through September 24, 2010) will be listed.

It is also possible to create a text file containing a list of all files in the current directory and its subdirectories, although be aware that this could be a long list.

**To create a listing of all files in a directory and its subdirectories**

1. Click Start, and then click Run. In the Run box, type cmd, and then press Enter.
2. Change to the directory to be documented.
3. At the command prompt, type the following command, and then press Enter:

dir /s /-c /o:-d /t:c /q > FileList.txt

Executing this command creates a text file called FileList.txt in the current directory, which should be copied to a removable media for further examination.

Note   There are ways to create such a list using other tools and scripts. However, the goal of this section is to assist in gathering information quickly using tools that are known to be available on the computer. If there has been time to prepare an emergency response toolkit that contains a more advanced script, use it instead of the procedure shown here.

After this search is complete, sort the results by type to assist in identifying the executable files, which are typically the malware target. The following list provides examples of some of the more common file types that can contain executable code:

|  |  |  |  |
| --- | --- | --- | --- |
| \*.exe | \*.html | \*.cmd | \*.htm |
| \*.bat | \*.cpl | \*.pif | \*.pot |
| \*.vbs | \*.vbe | \*.js | \*.jse |
| \*.scr | \*.jpg | \*.doc | \*.xls |
| \*.mdb | \*.com | \*.ocx |  |

Note   The search list may contain a large number of entries, and there may not be time to review all modifications at this stage in the process. However, it is important to save or print a copy of this list when there is sufficient time to review the likely target files.

If the person performing the task is unsure of a particular file name, an Internet search can sometimes indicate the nature of a file and whether it has been linked to malware. However, it is important that such a search be performed on a system that is not infected, because Internet browsing behavior can be modified by a malware attack.

Also, it is important to be aware that a number of malware attacks have used valid system file names but have placed the file in a different folder to avoid detection by the Windows File Protection service. For example, one file that has been used in the past by malware is Svchost.exe, which is normally installed and protected in the %WINDIR%\System32 folder. However, examples of malware creating a file of the same name directly in the %WINDIR% folder have been seen. It is important to check the full path as well as the file names.

Some of the common target areas for malware attacks to place and modify files include:

* %Windir% and %SystemRoot%. These variables are assigned to the Windows operating system default installation folder. This folder contains a number of important executable and configuration files. By default, this variable will point to the following folder paths:
* C:\Windows (for Windows 7, Windows Vista, and Windows Server 2008)
* C:\Winnt\ (for Microsoft Windows NT®/Windows 2000 or systems that were upgraded)
* %Temp% and %TMP%. These variables are assigned to the path used by applications to write temporary files. By default, this variable is assigned to the following paths:
* C:\WINNT\Temp (for Windows NT/Windows 2000 systems)
* C:\Document and Settings\User\_Name\Local Settings\Temp (for Windows XP and Windows Server 2003)
* C:\Users\User\_Name\AppData\Local\Temp (for users of Windows Vista and later versions of Windows)
* C:\Windows\Temp (for the built-in system account in Windows Vista and later versions of Windows)

If examination of the files on the system uncovers any infected files, copy the files to removable media for future examination. Because these files are infected, steps should be taken to ensure they are not available for anything other than the intended process. Consider these steps to assist in protecting these copies:

* Change the file name extension. By changing the file name’s extension to something unknown to the operating system, it will not be able to execute the file by an accidental click. For example, consider replacing the last letter of the file *Avirus.exe* with an underscore to make it Avirus.ex\_.
* Store the infected files in a protected archive. Consider compressing the files that are infected and using a password to protect the compressed file.
* Use specialized media. Ensure that the removable media are physically identifiable from standard media by using colored disks or nonstandard labels.
* Lock files in a safe place. Physically secure all malware sample media in a safe or some other secure storage facility.
* Send only protected archives. If it is necessary to send suspected malware through email (for example, to an antimalware vendor), always send a password-protected archive file of the malware. Email gateways will be able to scan and detect the malware if it is sent as a typical unprotected attachment.

Note   Some malware attacks have used protected archives to escape antimalware scanning techniques. As a result, a number of organizations have blocked or quarantined all inbound archived files. Ensure this mechanism will work for the intended recipient before sending the file.

### Users and Groups

Some malware attacks will try to elevate the privileges of existing users on the system or add new accounts in groups that have administrator privileges. Check for the following unusual settings:

* Odd user accounts and groups
* User names that do not appear to fit
* Groups that contain invalid user membership
* Invalid user rights
* Recently elevated privileges for any user or group accounts

Confirm that all Administrator group members are valid. Use the Local Users and Groups Microsoft Management Console (MMC) snap-in to check for any unusual additions to the local Administrators group. Also check the security log of the local computer for any unusual entries. For example, Account Management category entries such as event 636 indicate that a new member has been added to a local group. These logs will also provide the date and time that the change took place.

If the system being examined is running a Windows Server operating system, use the Active Directory® Users and Groups MMC snap-in to examine the domain group memberships, as well. For more information about well-known security identifiers and their associated user and group information, see the Microsoft Support article, “Well-known security identifiers in Windows operating systems” at <http://support.microsoft.com/?kbid=243330>.

### Shared Folders

Another common symptom of malware is the use of shared folders to spread infection. Check the state of the shared folders on the infected system using the Computer Management MMC snap-in or via the command line using the NetShare command. The following tables illustrate the default shares on Windows clients and servers.

Note   By default, Microsoft Windows 9*x* computers do not share files or folders unless file sharing has been enabled. Also, Windows 9*x* clients do not have admin$ or equivalent hidden shares; only those folders or volumes that are specifically shared are available via the network (barring the system being compromised some way or some remote-control software being installed on it).

Table B-1. Windows 7 Default Folder Shares

| Shared folder | Shared path | Comment |
| --- | --- | --- |
| ADMIN$ | C:\Windows | Remote Admin |
| C$ | C:\ | Default share |
| n$ | n:\ | Represents a share for the root of each fixed drive on the system |
| SharedDocs | C:\Users\Public\Documents | Will be added if local file sharing has been enabled |

Table B-2. Windows Server 2008 R2 Default Folder Shares

| Shared folder | Shared path | Comment |
| --- | --- | --- |
| ADMIN$ | C:\Windows | Remote Admin |
| C$ | C:\ | Default share |
| n$ | n:\ | Represents a share for the root of each fixed drive on the system |
| SharedDocs | C:\Users\Public\Documents | Will be added if local file sharing has been enabled |
| wwwroot$ | C:\inetpub\wwwroot | Will be set up if Microsoft Internet Information Services has been installed as a Web server |

The permissions on these shares can be examined with the SrvCheck command-line tool, available as part of the Windows Server 2003 Resource Kit Tools at [www.microsoft.com/downloads/en/details.aspx?familyid=9d467a69-57ff-4ae7-96ee-b18c4790cffd&displaylang=en](http://www.microsoft.com/downloads/en/details.aspx?familyid=9d467a69-57ff-4ae7-96ee-b18c4790cffd&displaylang=en).

### Opened Network Ports

Many malware attacks attempt to weaken a compromised system to make it easier to attack in the future. One often-used technique is to open network ports on the host that are then used by the malware attacker to gain an additional route to the host.

A number of tools can be used to export a list of the current network port settings, including PortQRY. For more information about this tool, see PortQry Command Line Port Scanner Version 2.0 at [www.microsoft.com/downloads/en/details.aspx?familyid=89811747-C74B-4638-A2D5-AC828BDC6983](http://www.microsoft.com/downloads/en/details.aspx?familyid=89811747-C74B-4638-A2D5-AC828BDC6983) and the Microsoft Support article, “New features and functionality in PortQry version 2.0,” at <http://support.microsoft.com/?kbid=832919>.

Another tool is the FPort command-line utility from Foundstone, available at [www.foundstone.com](http://www.foundstone.com). In addition, if the computer is using a personal firewall, such as Windows Firewall or Zone Labs ZoneAlarm, check the documentation that came with the firewall, because many of them can also show listening ports and the applications that are listening on them.

Finally, the Netstat command-line utility that comes with Windows to document the state of current network connections and network ports that are listening can be used. This tool can be used to obtain a complete printout of the network connections and port status.

**To create a Netstat report**

* On the infected host, click Start, and then click Run. In the Run box, type the following command, and then press Enter:

Netstat -an >c:\netstat\_report.txt

Note   If Netstat is running on Windows XP or a later Windows operating system, it may be helpful to use the following command, which will also list the associated process identifier in the report:

Netstat –ano >c:\netstat\_report.txt

A text file called netstat\_report.txt (it may also be useful to add the date to the file name) will be created in the root of drive C. This file should be saved to a removable media for future examination.

#### Using a Network Protocol Analyzer

A network protocol analyzer tool or sniffer can be used to create a network traffic log of data being transmitted to and from the infected host. The network trace file should be saved as part of the set of information files for future examination.

Examples of network protocol analyzers that are used for creating these network trace files include the Microsoft Network Monitor, available at [www.microsoft.com/downloads/en/details.aspx?displaylang=en&FamilyID=983b941d-06cb-4658-b7f6-3088333d062f](http://www.microsoft.com/downloads/en/details.aspx?displaylang=en&FamilyID=983b941d-06cb-4658-b7f6-3088333d062f), or non-Microsoft tools such as the Wireshark packet analyzer, available at [www.wireshark.org](http://www.wireshark.org).

### System Event Logs

It may be possible to use the Windows system event logs to spot a wide range of unusual behavior that could be used to identify both the changes malware has made and when they were made. Use the Event Viewer management console to save each type of event log file (Application, Security, and System) to removable media for further examination. By default, these files are stored in C:\Winnt\System32\Config\ and are called AppEvent.evt, SecEvent.evt, and SysEvent.evt. However, while the system is active, these files are locked and should be exported using the Event Viewer management tool.

The following tips provide information on how these logs can be used to help determine the effects of a malware attack:

* Look for any changes at the time of the suspected attack.
* Compare event log times with file creation and modification times .
* Look for accounts that were created or had a password changed around the time of a suspected intrusion.

At the end of the malware examination process, it may be possible to consider reconnecting the isolated networks, depending on the nature of the malware. For example, if the examination determines that the malware spreads only via a particular peer-to-peer application, changing the perimeter firewall filters to block the network ports used by this application allows the networks and other services to be restored. Such a remedy enables the organization to return to some level of normal communications while the system recovery process is undertaken.

## Task 4: Evaluate the Data

After the information has been gathered, the support technician should evaluate the collected data against the following set of questions to help determine whether a malware attack is a likely cause of the report:

* Could the report be the result of a legitimate new or updated characteristic of the system?
* Could it be explained by the activities of an authorized user (instead of a hacker/intruder)?
* Could it be explained by known system activity?
* Could it be explained by authorized changes to programs or systems?

Finally, a check should be made with Microsoft Malware Protection Center at [www.microsoft.com/security/portal](http://www.microsoft.com/security/portal) or other security vendors’ websites to determine whether this report matches some existing virus or worm alert.

## Task 5: Determine Whether the Issue Is Real

After the initial information has been gathered and used to determine the nature of the alert, it should be possible for the help desk to decide whether a false alarm, hoax, or real malware attack has occurred.

Creating a fake malware report is far easier than developing a virus or worm, which unfortunately assures the creation of many false malware alerts. These hoaxes and the calls and warnings they generate waste considerable time and money. Hoaxes also annoy users and tend to make them question the value of reporting potential attacks. The following considerations should be made to ensure the alert is correctly handled.

* False alarm. If the report is a false alarm, the call information should be logged. Periodic review of this information may help determine whether additional user training is required.
* Hoax. It is important to track and record false malware alerts as well as real malware activity, as they are still attack instances—they just do not use malicious code. Communicating information about false malware alerts as well as real malware threats to users should be part of the organization’s regular antimalware communications. This information will help the users recognize hoaxes in advance and therefore reduce lost productivity.
* Known infection. If the system appears to be infected, the help desk should take steps to determine whether the infection is a known attack that can be handled with an existing antimalware application. The system’s antimalware application should be checked to ensure that it is operational and up to date. A complete system scan should then be undertaken to attempt to clean the system. If this scan successfully identifies and cleans the infection, the call should be logged and a warning sent to all users to ensure their antimalware systems are running correctly and updated. If the scan fails to identify a specific form of malware, it should be considered a new infection and the guidance in the Introduction to Malware Response section followed.
* New infection. If the system appears to be infected by a new malware attack, a number of initial actions should be followed to help ensure the problem is communicated in the correct manner. These initial actions are designed to help the IT support staff consistently follow a process that ensures the correct course of action is followed. Answers to the initial questions listed earlier will help determine which of the following initial actions should be considered at this stage:
* Contact the assigned member of the emergency response team with details of the alert.
* If the suspect computer is a server, contact its administrator to discuss the implications of removing the computer from the network.
* If the suspect computer is a workstation, contact its users to discuss the implications of removing the computer from the network.
* Consider triggering a high-level alert or warning of the detected attack to users of the IT system.

At this point, the role of the help desk is complete. Responsibility for the outbreak moves to the incident response process, and the members of the Computer Security Incident Response Team need to be notified.

If the outbreak has been detected in the antimalware community, use the guidance provided by the organization’s antimalware vendor to help determine the severity of the outbreak. If the outbreak is currently unknown in the wider antimalware community, report the incident to the organization’s antimalware vendor as soon as possible.

For more information, see the Microsoft malware submission form at <https://www.microsoft.com/security/portal/Submission/Submit.aspx>.

## Additional Reading

* Microsoft Malware Protection Center: [www.microsoft.com/security/portal/Threat/Threats.aspx](http://www.microsoft.com/security/portal/Threat/Threats.aspx)
* Responding to malware and vulnerabilities: <http://technet.microsoft.com/en-us/library/bb418932.aspx>
* Responding to IT Security Incidents: <http://technet.microsoft.com/en-us/library/cc700825.aspx>
* Microsoft Support article, “Well-known security identifiers in Windows operating systems”: <http://support.microsoft.com/?kbid=243330>
* Microsoft Support article, “How to use the System Configuration utility to troubleshoot configuration errors in Windows Vista”: <http://support.microsoft.com/kb/950093>
* Microsoft Support article, “How to troubleshoot configuration errors by using the System Configuration utility in Windows XP”: <http://support.microsoft.com/kb/310560>
* Sysinternals: <http://technet.microsoft.com/sysinternals>
* Sysinternals Utilities Index: <http://technet.microsoft.com/en-us/sysinternals/bb545027.aspx>
* Windows Server 2003 Deployment Guide: <http://technet.microsoft.com/en-us/library/cc739492(WS.10).aspx>

# Appendix C: Create an Offline Scanning Kit

This appendix offers three approaches to creating a tool for offline scanning:

* Using the Microsoft Diagnostics and Recovery Toolset (DaRT), part of the Microsoft Desktop Optimization Pack (MDOP): [www.microsoft.com/windows/enterprise/products/mdop/dart.aspx](http://www.microsoft.com/windows/enterprise/products/mdop/dart.aspx).
* Using Windows PE from the Windows Automated Installation Kit (Windows AIK): <http://technet.microsoft.com/en-us/library/dd349343(WS.10).aspx>.
* Using MDT: <http://technet.microsoft.com/en-us/solutionaccelerators/dd407791.aspx>.

Each approach results in a bootable CD-ROM or DVD with one or more tools for removing malware from a compromised system. All have advantages and disadvantages, so select whichever approach best meets the needs and available resources in the organization.

DaRT is the simplest to implement. It is included with MDOP, which is available only to organizations that have a contract that includes Microsoft Software Assurance.

Both the Windows PE and MDT approaches are based entirely on free software. The Windows PE solution is more time-consuming to maintain, because the disc image file has to be created from scratch each time any of its files require updating, but it is a proven solution that has been used by thousands of organizations and individuals since its original publication in 2007.

When properly deployed, MDT automates much of the image building process; the image can be updated or tools can be added to the image without having to rebuild it from scratch, and the MDT solution can be configured to boot off of the network using PXE in addition to a CD-ROM or DVD. The only drawback to MDT is it may take more time to set up the initial disc image if non-Microsoft device drivers and operating system updates are included.

Figure C-1 summarizes the decisions to be made when determining which approach to choose.

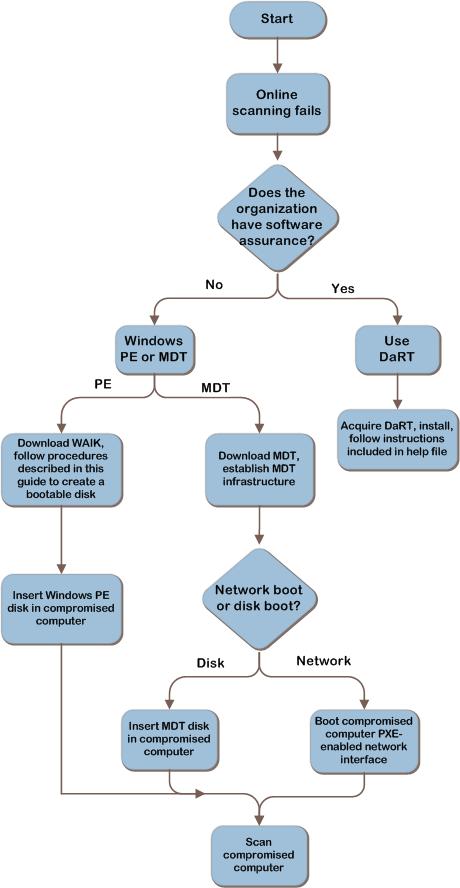


Figure C-1. Determine which approach to use to create offline scan tool kit

## Option 1: Microsoft Diagnostics and Recovery Toolset

DaRT is a component of MDOP available to Microsoft Volume Licensing customers who have Software Assurance. DaRT starts the computer from a CD or DVD to enable administrators to perform an offline examination and repair of severe operating system problems. DaRT includes Standalone System Sweeper, a comprehensive antimalware and antispyware utility that is particularly effective at removing malware that tries to hide itself using rootkit technology. More information is available at [www.microsoft.com/windows/enterprise/products/mdop/dart.aspx](http://www.microsoft.com/windows/enterprise/products/mdop/dart.aspx).

## Option 2: Windows Preinstallation Environment

Windows PE provides powerful preparation and installation tools for Windows operating systems. With Windows PE, Windows can be started from a removable disk, which provides resources to troubleshoot Windows on the client computer. For more information about Windows PE, download the Windows Preinstallation Environment Technical Overview at <http://download.microsoft.com/download/5/b/5/5b5bec17-ea71-4653-9539-204a672f11cf/WindowsPE_tech.doc>.

### Unsupported Tools and Technologies

Windows PE has the following limitations relative to tools and technologies:

* It does not support Internet Explorer.
* It supports Distributed File System (DFS) name resolution only to stand-alone DFS roots.
* Files or folders on a computer running Windows PE cannot be accessed from another computer. In other words, the Server service is not available within Windows PE.
* It supports both Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6), but it does not support other protocols, such as Internetwork Packet Exchange/Sequenced Packet Exchange.
* It does not support the Microsoft .NET Framework.
* It does not support applications packaged with Windows Installer (.msi).
* Because it does not support Windows on Windows, 16-bit applications will not run in 32-bit versions of Windows PE, and 32-bit applications will not run in 64-bit versions of Windows PE.
* It cannot access encrypted volumes such as those protected with BitLocker.
* It only supports local drives formatted with the File Allocation Table (FAT) and NTFS file system.

Windows PE also has these limitations:

* To prevent its use as a general-purpose operating system, Windows PE automatically restarts after 72 hours of continuous use.
* Windows PE includes only a subset of the Windows Vista Win32® application programming interfaces (APIs), including I/O (disk and network) and core Win32 APIs. More information about adding network drivers can be found in the [Windows Preinstallation Environment Technical Overview](http://download.microsoft.com/download/5/b/5/5b5bec17-ea71-4653-9539-204a672f11cf/WindowsPE_tech.doc) at <http://download.microsoft.com/download/5/b/5/5b5bec17-ea71-4653-9539-204a672f11cf/WindowsPE_tech.doc>.
* Applications that require any of the following Win32 APIs will not run in Windows PE: access control, NetShow Theater Administration, OpenGL, power options, printing and print spooler, still image, tape backup, terminal services, user profile, Windows station and desktop, Windows multimedia, and the Windows shell.

### Prerequisites

The following are operating system and feature requirements for preparing a Windows PE kit:

* Windows 7, Windows Vista with SP1, Windows Vista with SP2, Windows Server 2008, Windows Server 2008 R2, or Windows Server 2003 R2.
* DVD burner and software to write to a CD-ROM.
* 1,707 megabytes (MB) of free space on the computer’s hard disk to download the Windows PE .img file.

Note   An additional 800 MB of space is required for the boot image on drive C of the computer when using the default script for the kit.

For more information about 32-bit and 64-bit system requirements, see the Windows PE Technical Reference at <http://technet.microsoft.com/en-us/library/dd744322(WS.10).aspx>.

### Task Overview

Complete the following tasks to prepare an offline scanning kit to conduct offline scans:

1. Install Windows AIK.
2. Download the malware scanning tools and utilities.
3. Create the Offline Scanning Kit CD-ROM.
4. Use the Offline Scanning Kit to scan the target computer.

### Task 1: Install Windows AIK

The first task in this process is to obtain Windows AIK. This kit includes Windows PE and other files to be installed on the computer. The kit installs by default as an image (\*.img) file on any system drive chosen.

NoteWindowsAIK supports both Windows Vista and Windows 7.

**To install Windows AIK on a computer**

1. Download Windows AIK from the Microsoft Download Center at [www.microsoft.com/downloads/details.aspx?familyid=696DD665-9F76-4177-A811-39C26D3B3B34](http://www.microsoft.com/downloads/details.aspx?familyid=696DD665-9F76-4177-A811-39C26D3B3B34).

NoteThe size of the .img file for Windows AIK is 1,707 MB. For this reason, extended time to download the file may be required, depending on the connection speed to the Microsoft Download Center.

1. Burn the ISO file for Windows AIK to a DVD.
2. On the Windows AIK DVD that was created, double-click StartCD.exe to install Windows AIK on the target computer.

### Task 2: Download the Malware Scanning Tools and Utilities

The tools that will be used with Windows PE to perform malware scans on the target computer will need to be identified. Windows PE does not support tools that use .msi packages to install on computers. In addition, the amount of RAM on the target computer can constrain what scanning tools can be used.

A number of antimalware tools are available for free that require no installation and can be run as program files in the Windows PE environment. These tools can also be run from a USB device.

Download the malware scanning tools that will be used to a temporary location on the target computer.

ImportantSome antimalware tools require network access to run. For this reason, only use antimalware tools that are available to use offline when this guidance is used to create an offline scanning kit CD-ROM. Microsoft recommends reading the installation instructions for all of the offline scanning tools that will be used. Some tools may not be compatible with all Windows operating systems.

At the time this guidance was written, the following tools ran with Windows PE on a computer running Windows 7 or Windows Vista with at least 512 MB of RAM:

* McAfee AVERT Stinger, a stand-alone virus scanner from McAfee: [www.mcafee.com/us/downloads/free-tools/stinger.aspx](http://www.mcafee.com/us/downloads/free-tools/stinger.aspx). This tool is available for offline use. The signature files for the tool will be as current as the download date listed.
* Spybot—Search & Destroy: [www.safer-networking.org/en/spybotsd](http://www.safer-networking.org/en/spybotsd). Factors to note about this tool are:
* Before this tool can be used, it must first be installed in the Windows PE session, and then the latest signature file detection updates from Spybot within the same session must be installed. After the tool is installed, it will start by default from X:\Program Files\Spybot—Search & Destroy\spybotsd unless a different path was specified during installation.
* The signature files for the tool will be as current as the download date listed; the signature files can be updated from within Spybot—Search & Destroy.
* When this tool is executed, it can be forced to scan all registry hives, including those from the inactive operating system, by executing it with the /allhives parameter—for example, X:\Program Files\Spybot—Search & Destroy\spybotsd /allhives.

For more information about using this tool, see the Tutorial page of the Spybot website.

* The following utilities are designed to help manage the target computer while in the process of removing malware from it:
* Drive Manager at [www.alexnolan.net/software/driveman.htm](http://www.alexnolan.net/software/driveman.htm) from the Portable Freeware Utilities by Alex Nolan website at [www.alexnolan.net/](http://www.alexnolan.net/). This tool identifies different drive types, such as hard drives, CD/DVD drives, USB drives, and network drives, and lists their properties for examination. This tool is available for offline use.
* System Spec at [www.alexnolan.net/software/sysspec.htm](http://www.alexnolan.net/software/sysspec.htm) from the Portable Freeware Utilities by Alex Nolan website provides information about the current hardware on the computer. This tool may be useful if it is required to provide detailed information about the hardware while the computer is being serviced. This tool is available for offline use.

### Task 3: Create the Offline Scanning Kit CD-ROM

Creating the offline scanning kit CD-ROM requires that a 32-bit Windows PE image be produced for the kit and that the base Windows PE image be modified by adding the tools to it. The size of the disk cache will then need to be changed to provide some additional space for RAM, and an ISO image file will need to be built to burn the changed image to a CD-ROM. Although these tasks can be performed on either 32-bit or 64-bit versions of Windows, the Windows PE image must be 32 bit. Periodically, the latest virus signature updates will need to be downloaded for the offline scanning tools on the CD-ROM to keep them as effective as possible to detect malware.

ImportantAfter the creation of the Windows PE image has started, it is important to complete all of the steps in this task without interruption. If the tools that will be used have already been downloaded, this process should take about 30 minutes to finish, depending on the system’s performance and whether the steps in this task have been performed exactly as prescribed. About 800 MB of free space will be needed on drive C to complete this procedure. Ensure that all drive letter references are updated as needed.

**To create an offline scanning kit CD-ROM**

1. Log on to the computer as an administrator, right-click Deployment Tools Command Prompt, point to Run as administrator, and then click Continue.

NoteThis step applies to Windows Vista and later versions of Windows. If Windows XP is running on the target computer, click Start, and then point to All Programs. Point to Microsoft Windows AIK, and then click Windows PE Tools Command Prompt.

1. At the command prompt, type the following command, and then press Enter to create a copy of the x86 image of Windows PE and set up a working folder directory on the computer:

copype x86 c:\WinPE

1. At the command prompt in the new directory C:\WinPE, type the following command, and then press Enter to mount the WinPE.wim image so that it can be changed:

imagex /mountrw winpe.wim 1 c:\WinPE\Mount

1. At the command prompt, type the following command, and then press Enter to access the registry subkey:

reg load HKLM\\_WinPE\_SYSTEM c:\WinPE\Mount\windows\system32\config\system

1. At the command prompt, type the following command, and then press Enter to create a 96-MB disk cache of RAM:

reg add HKLM\\_WinPE\_SYSTEM\ControlSet001\Services\FBWF /v WinPECacheThreshold /t REG\_DWORD /d 96 /f

1. At the command prompt, type the following command, and then press Enter to exit this registry key:

reg unload HKLM\\_WinPE\_SYSTEM

1. Create a directory for the malware scanning tools under the Mount folder (for example, Tools could be used to name this folder).

mkdir c:\WinPE\mount\Tools

1. Copy the tool files that that were downloaded in Task 2 to the tools directory just created—for example:

copy <tools from the Task 2 directory> c:\WinPE\mount\Tools

1. At the command prompt, type the following command, and then press Enter to save the changes:

imagex /unmount c:\WinPE\Mount /commit

1. At the command prompt, copy the following command, press Enter, and then type Yes to overwrite the existing file:

copy c:\WinPE\WinPE.wim c:\WinPE\ISO\sources\boot.wim

1. At the command prompt, type the following command, and then press Enter to create an ISO file of the Windows PE image:

oscdimg -n -bc:\WinPE\etfsboot.com c:\WinPE\ISO c:\WinPE\Malware\_Removal\_x86.iso

1. Burn the ISO file located at C:\WinPE\Malware\_Removal\_x86.iso to a CD-ROM, and then test the Windows PE image to verify that it runs all of the malware scanning tools correctly.

NoteWindows Virtual PC can also be used at [www.microsoft.com/windows/virtual-pc](http://www.microsoft.com/windows/virtual-pc) to test the image.

The CD-ROM for the offline scanning kit is now ready. If more frequent virus signature updates are required for the environment, Microsoft recommends maintaining the chosen scanning tools on a USB device to obtain the latest updates. For more information about Windows PE and the Windows AIK, download the Windows Preinstallation Environment Technical Overview at <http://download.microsoft.com/download/5/b/5/5b5bec17-ea71-4653-9539-204a672f11cf/WindowsPE_tech.doc>, the *Windows Automated Installation Kit User’s Guide* (WAIK.chm), and the *Windows PE User’s Guide* (WinPE.chm) that is installed with the Windows AIK.

### Task 4: Use the Offline Scanning Kit to Scan the Target Computer

Now the Windows PE image and the tools that were selected to scan the computer for malware are ready to use.

To use the Windows PE CD-ROM and tools to scan the target computer

1. Place the new CD-ROM in the computer’s CD drive or DVD drive, and then ensure that the computer is started from this drive according to the computer's startup order.

Option: Insert the USB device in a slot on the computer to ensure that the device is loaded when the operating system is started.

NoteThe basic input/output system (BIOS) settings for the startup order of the computer may need to be configured to enable the computer to boot from the CD or DVD drive. Refer to the computer manufacturer or BIOS manufacturer for instructions on how to do so.

1. Run the selected malware scanning tools. If the default configuration information in Task 3 was used to build the Windows PE image, the tools will be located at X:\Tools. The listed tools can be run by typing the name of the program file for each one at the command prompt.

Option: If a USB device was used to provide updated signatures or tools, and the drive letter that the USB device is using is unknown, the drive letter can be determined using Drive Manager, which is located at X:\Tools.

NoteTo run Spybot, refer to Spybot’s installation instructions, and ensure that the definition program file runs after this tool is installed on the computer.

CautionRunning malware scanning tools on an infected computer may damage the computer’s ability to start properly. If key boot files are infected by malware, the cleaning process may prevent the operating system from working. For this reason, it is important to regularly back up all important information files on the computer. In addition, after restoring these files to the computer from the backup resource, Microsoft recommends rescanning the computer to detect any malware that may be present in the backup files.

## Option 3: Microsoft Deployment Toolkit

MDT 2010 is the latest version of MDT, a Solution Accelerator for operating system and application deployment. MDT 2010 supports deployment of Windows 7 and Windows Server 2008 R2 in addition to deployment of Windows Vista, Windows Server 2008, Windows Server 2003, and Windows XP.

In addition to operating system and application deployment, MDT 2010 can be used to easily create and manage Windows PE boot images including all of the latest security patches, network drivers, and hard disk drivers. This section describes how to use MDT 2010 to create an offline scanning kit WIM and CD-ROM.

### Prerequisites

The following are software requirements for using MDT 2010 to create an offline scanning kit WIM and CD-ROM:

* Windows 7, Windows Vista with SP1, or Windows Server 2008
* DVD burner and software to write to a CD-ROM
* 1,707 MB of free space on the computer's hard disk drive to download the Windows PE .img file

NoteAn additional 800 MB of space is required for the boot image on drive C of the computer when using the default script for the kit.

### Task Overview

Complete the following tasks to create an offline scanning kit CD-ROM with MDT 2010:

1. Install MDT 2010.
2. Install Windows AIK for Windows 7.
3. Download the malware scanning tools and utilities.
4. Configure MDT 2010.
5. Create an Offline Scanning Kit CD-ROM.
6. Use the Offline Scanning Kit to scan a computer.

### Task 1: Install MDT 2010

**To install MDT 2010, complete the following steps**

1. Download MDT 2010 at <http://go.microsoft.com/fwlink/?LinkId=159061>.
2. Double-click MicrosoftDeploymentToolkit\_x86.msi or MicrosoftDeploymentToolkit\_x64.msi, and then click Install.
3. On the Welcome to the Microsoft Deployment Toolkit 2010 Setup Wizard page, click Next.
4. On the End-User License Agreement page, review the license agreement, select I accept the terms in the License Agreement, and then click Next.
5. On the Custom Setup page, click Next.
6. Click Install.

The Installing Microsoft Deployment Toolkit page appears. The installation process status is displayed and eventually finishes.

1. On the Completing the Microsoft Deployment Toolkit Setup Wizard page, click Finish.

### Task 2: Install Windows AIK for Windows 7

The first task in this process is to obtain the Windows AIK for Windows 7. This kit includes Windows PE and other files to be installed on the target computer. By default, the kit is installed as an image (\*.img) file on any system drive chosen.

NoteThe Windows AIK supports both Windows Vista with SP1 and Windows 7.

To install the Windows AIK on the computer

1. Download the Windows AIK from the Microsoft Download Center at [www.microsoft.com/downloads/details.aspx?familyid=696DD665-9F76-4177-A811-39C26D3B3B34&displaylang=en](http://www.microsoft.com/downloads/details.aspx?familyid=696DD665-9F76-4177-A811-39C26D3B3B34&displaylang=en).

NoteThe size of the .img file for the Windows AIK is 1,707 MB. For this reason, extended time may be required to download the file, depending on the connection speed to the Microsoft Download Center.

1. Burn the .img file for the Windows AIK to a DVD.
2. On the Windows AIK DVD that was created, double-click StartCD.exe to install the Windows AIK on the computer.
3. Select Windows AIK Setup from the menu on the left side of the Welcome to Windows Automated Installation Kit page.
4. Follow the prompts in the installation wizard to install the Windows AIK.

### Task 3: Download the Malware Scanning Tools and Utilities

This task is identical to the steps described in Task 2 of Option 2: Windows Preinstallation Environment.

### Task 4: Configure MDT 2010

Now that MDT is installed, a deployment share needs to be created and drivers and security patches should be added to the deployment share.

**To create a deployment share**

1. Click Start, and then point to All Programs. Point to Microsoft Deployment Toolkit, and then click Deployment Workbench.
2. In the Deployment Workbench console tree, go to Deployment Workbench/Deployment Shares.
3. In the console tree, right-click Deployment Shares, and then click New Deployment Shares to start the New Deployment Share Wizard.
4. Complete the wizard using the information in Table C-1.

Table C-1. Information for Completing the New Deployment Share Wizard

| Wizard page | Action |
| --- | --- |
| Path | * Click Browse. * In the Browse for folder dialog box, create C:\Deploymentshare$, and then click OK. * Click Next. |
| Share | Click Next. |
| Descriptive Name | Click Next. |
| Allow Image Capture | Click Next. |
| Allow Admin Password | Click Next. |
| Allow Product Key | Click Next. |
| Configure User State | Click Next. |
| Summary | Click Next. |
| Confirmation | Click Finish. |

The New Deployment Share Wizard finishes, and the new deployment share—MDT Deployment Share (C:\DeploymentShare$)—appears in the details pane.

**To add drivers**

1. Click Start, and then point to All Programs. Point to Microsoft Deployment Toolkit, and then click Deployment Workbench.
2. In the Deployment Workbench console tree, go to Deployment Workbench/Deployment Shares/MDT Deployment Share (C:\DeploymentShare$)/Out-of-Box Drivers.
3. In the Actions pane, click Import Drivers to start the Import Driver Wizard.
4. Complete the Import Driver Wizard using the information in Table C-2.

Table C-2. Information for Completing the Import Driver Wizard

| Wizard page | Action |
| --- | --- |
| Specify Directory | In Driver source directory, type driver\_path (where driver\_path is the fully qualified path to the folder containing the device drivers), and then click Next. |
| Summary | Click Next. |
| Confirmation | Click Finish. |

The Import Driver Wizard finishes. The device drivers are added to the list of operating systems in the details pane and are copied to the deployment\_share\Out-of-box Drivers folder (where deployment\_share is the deployment share that was created earlier).

**To import packages (security fixes)**

1. Click Start, and then point to All Programs. Point to Microsoft Deployment Toolkit, and then click Deployment Workbench.
2. In the Deployment Workbench console tree, go to Deployment Workbench/Deployment Shares/deployment\_share/Packages (where deployment\_share is the name of the deployment share where the application will be added).
3. In the Actions pane, click Import OS Packages to start the Import OS Packages Wizard.
4. Complete the Import OS Packages Wizard using the information in Table C-3.

Table C-3. Information for Completing the Import OS Packages Wizard

| Wizard page | Action |
| --- | --- |
| Specify Directory | In Package source directory, type path (where path is the fully qualified path to the folder that contains the package to be imported), and then click Next.  Note   Alternatively, click Browse to find the folder on a local drive or network shared folder. |
| Summary | View the information in the Details box, and then click Next. |
| Confirmation | Tip   Click Save Output to save the output of the wizard to a file. Also, View Script can be clicked to view the Windows PowerShell® scripts used to perform the wizard tasks.  Click Finish. |

The Import OS Packages Wizard finishes. The package is added to the list of packages in the details pane, and the deployment\_share\Packages\package\_type\package\_name folder is created (where deployment\_share is the name of the deployment share, package\_type is the type of package that was added, and package\_name is name of the package that was added).

### Task 5: Create an Offline Scanning Kit CD-ROM

Now an offline scanning kit CD-ROM can be created.

**To create an offline scanning kit CD-ROM**

1. Click Start, and then point to All Programs. Point to Microsoft Deployment Toolkit, and then click Deployment Workbench.
2. In the Deployment Workbench console tree, expand the Deployment Workbench node, and then click Deployment Shares.
3. In the details pane, click deployment\_share (where deployment\_share is the name of the deployment share).
4. In the Actions pane, click Properties to open the ***deployment\_share*** Properties dialog box.
5. On the Windows PE x86 Settings tab, select Generate a Generic Windows PE WIM File.

Note   Although these tasks can be performed on either 32-bit or 64-bit versions of Windows, the Windows PE image must be 32 bit.

1. Specify an Image Description of Offline Scanning Kit.
2. Select Generate a generic bootable ISO image.
3. Specify an ISO file name, such as Malware\_Removal\_x86.iso.
4. In Extra Directory to Add, specify the path to the malware tools created in Task 3.
5. Change the scratch space size to 128, and then click OK.
6. Right-click Deployment Share, choose Update Deployment Share, and then click Next.
7. Click Next, and then click Finish.
8. Burn the ISO file located at C:\DeploymentShare\Boot folder\Malware\_Removal\_x86.iso to a CD-ROM, and then test the Windows PE image to verify that it runs all of the malware scanning tools correctly.

Note   Windows Virtual PC at [www.microsoft.com/windows/virtual-pc](http://www.microsoft.com/windows/virtual-pc) can also be used to test the image.

The CD-ROM for the offline scanning kit is now ready.

### Task 6: Use the Offline Scanning Kit to Scan a Computer

Now the Windows PE image and the tools that were selected to scan the computer for malware are ready. If the computer to be scanned is PXE capable, MDT can also be configured to start the computer over the network. For more information about this approach, refer to the MDT documentation.

**To use the Windows PE CD-ROM and tools to scan the computer**

1. Place the new CD-ROM in the computer’s CD drive or DVD drive, and then ensure that the computer has been started from this drive according to the computer's startup order.

Note   The BIOS settings for the startup order of the computer may need to be configured to enable the computer to start from the CD or DVD drive. Refer to the computer manufacturer or BIOS manufacturer for instructions on how to do so.

1. Run the malware scanning tools that were selected. If the default configuration information in Task 3 was used to build the Windows PE image, the tools will be located at X:\—that is, the root of drive X. The listed tools can be run by typing the name of the program file for each one at the command prompt.

Note   To run Spybot, refer to Spybot’s installation instructions, and ensure that the definition program file runs after installing this tool on the computer.

Caution   Running malware scanning tools on an infected computer may damage the computer's ability to start properly. If key boot files are infected by malware, the cleaning process may prevent the operating system from working. For this reason, it is important to regularly back up all important information files on the computer. In addition, after restoring these files to the computer from the backup resource, Microsoft recommends rescanning the computer to detect any malware that may be present in the backup files.

# Version History

|  |  |  |
| --- | --- | --- |
| **Version** | **Description** | **Date** |
| 1.1 | Minor updates to reflect current template. | November 2011 |
| 1.0 | First release. | February 2011 |

# Acknowledgments

The Solution Accelerators team acknowledges and thanks the people who produced the *Infrastructure Planning and Design Guide for Malware Response* as well as the *Malware Removal Starter Kit Guide* that preceded it*.* The following people were either directly responsible for or made a substantial contribution to the writing, development, and testing of this guide.

Content Developers:

* Jude Chosnyk – *GrandMasters*
* John Cobb – Wadeware LLC
* Mike Danseglio – *Microsoft*
* Charles Denny – *Microsoft*
* Kurt Dillard – *kurtdillard.com*
* Richard Harrison – Content Master Ltd.
* Paul Henry – Wadeware LLC
* Mike Kaczmarek – *Microsoft*
* Frank Simorjay – *Microsoft*
* Melissa Stowe – *Microsoft*
* Henry Webb – *Microsoft*

Editors:

* Michelle Anderson – Xtreme Consulting Group
* Laurie Dunham – *Xtreme Consulting Group*
* Jennifer Kerns – Wadeware LLC

Product Managers:

* Michelle Arney – *Microsoft*
* Alan Meeus – *Microsoft*
* Jim Stuart – *Microsoft*
* Michelle Walls – *Xtreme Consulting Group*

Program Managers:

* Tom Cloward – *Microsoft*
* Karina Larson – *Microsoft*

Test Team:

* Gaurav Singh Bora – *Microsoft*
* Raxit Gajjar – Infosys Technologies Ltd.
* Saurabh Garg – Infosys Technologies Ltd.
* Sumit Parikh – *Microsoft*
* Balkrishnan Venkiteswaran – *Infosys Technologies Ltd.*

|  |  |
| --- | --- |
| **Contributors and Reviewers:** | |
| * Cindy Agnew – Fife School District * Keith Alabaster – UK Civil Aviation Authority * Rich Benack – Microsoft * Rebecca Black – Microsoft * Anthony Blumfield – Microsoft * Mat Braverman – Microsoft * Derick Campbell – Microsoft * Chase Carpenter – Microsoft * Lander Casado – European Central Bank * Richard Chamama – DOROT, Inc. * Shiroy Choksey – Microsoft * Bret Clark – Microsoft * Steve Clark – Microsoft * Jennelle Crothers – Conservation & Liquidation Office * Jeremy Croy – Microsoft * Fidelis Ekezue – Microsoft * Dr. Barbara Endicott-Popovsky * Martin Fallenstedt – Microsoft * Joe Faulhaber – Microsoft * Tim Grootkerk – Capgemini * Karl Grunwald – Microsoft * Kelly Hengesteg – Microsoft * Robert Hensing – Microsoft * Kumi Hilwa – Microsoft * Eric Huggins – Pinnacle * Steve Jackson – PRTM * Adwait Joshi – Microsoft * Bashar Kachachi – Microsoft * JoAnne Kennedy – Microsoft | * Joseph Kessler * Russ Klanke * Jelle Komrij – Atos Origin * Oscar Kuenzli – Veleras International GmbH * Jimmy Kuo – Microsoft * Greg Lenti * John R Levins – Levins & Associates * Mike Lewis – Microsoft * Brad McCabe – Microsoft * Curtis Metz – Microsoft * Jeffrey Miller – Microsoft * Mark Miller – Microsoft * Anand V Venkat Narayana – Xinfotainment * Ranjeet Negi * Thom Nesbitt * Maareten Oosterink – Capgemini * Adam Overton – Microsoft * Daryl Pecelj – Microsoft * Sterling Reasor * Paul Schnackenburg – Expert IT Solutions * Ondrej Sevecek – GOPAS * Dan Sobel – Computer Wizardry * J. Andre Tournier – Take 5 Systems * Randy Treit – Microsoft * Max Uritsky – Microsoft * Othelo Vieira * Jeff Williams – Microsoft * Lee Yan – Microsoft |

## Feedback

Please direct questions and comments about this guide to [ipdfdbk@microsoft.com](mailto:ipdfdbk@microsoft.com?subject=IPD%20-%20Malware%20Response).