# Executive Summary

Malware, also known as malicious code, refers to a program that is covertly inserted into another program with the intent to destroy data, run destructive or intrusive programs, or otherwise compromise the confidentiality, integrity, or availability of the victim’s data, applications, or operating system. Malware is the most common external threat to most hosts, causing widespread damage and disruption and necessitating extensive recovery efforts within most organizations. Organizations also face similar threats from a few forms of non-malware threats that are often associated with malware. One of these forms that has become commonplace is phishing, which is using deceptive computer-based means to trick individuals into disclosing sensitive information.

This publication provides recommendations for improving an organization’s malware incident prevention measures. It also gives extensive recommendations for enhancing an organization’s existing incident response capability so that it is better prepared to handle malware incidents, particularly widespread ones. This revision of the publication, Revision 1, updates material throughout the publication to reflect the changes in threats and incidents. Unlike most malware threats several years ago, which tended to be fast- spreading and easy to notice, many of today’s malware threats are more stealthy, specifically designed to quietly, slowly spread to other hosts, gathering information over extended periods of time and eventually leading to exfiltration of sensitive data and other negative impacts.

Implementing the following recommendations should facilitate more efficient and effective malware incident response activities for Federal departments and agencies.

## Organizations should develop and implement an approach to malware incident prevention.

Organizations should plan and implement an approach to malware incident prevention based on the attack vectors that are most likely to be used currently and in the near future. Because the effectiveness of prevention techniques may vary depending on the environment (i.e., a technique that works well in a managed environment might be ineffective in a non-managed environment), organizations should choose preventive methods that are well-suited to their environment and hosts. An organization’s approach to malware incident prevention should incorporate policy considerations, awareness programs for users and information technology (IT) staff, vulnerability and threat mitigation efforts, and defensive architecture considerations.

## Organizations should ensure that their policies address prevention of malware incidents.

An organization’s policy statements should be used as the basis for additional malware prevention efforts, such as user and IT staff awareness, vulnerability mitigation, threat mitigation, and defensive architecture. If an organization does not state malware prevention considerations clearly in its policies, it is unlikely to perform malware prevention activities consistently and effectively throughout the organization. Malware prevention–related policy should be as general as possible to provide flexibility in policy implementation and to reduce the need for frequent policy updates, but should also be specific enough to make the intent and scope of the policy clear. Malware prevention–related policy should include provisions related to remote workers—both those using hosts controlled by the organization and those using hosts outside of the organization’s control (e.g., contractor computers, employees’ home computers, business partners’ computers, mobile devices).

## Organizations should incorporate malware incident prevention and handling into their awareness programs.

Organizations should implement awareness programs that include guidance to users on malware incident prevention. All users should be made aware of the ways that malware enters and infects hosts, the risks that malware poses, the inability of technical controls to prevent all incidents, and the importance of users in preventing incidents, with an emphasis on avoiding social engineering attacks. Awareness programs should also make users aware of policies and procedures that apply to malware incident handling, such as how to identify if a host may be infected, how to report a suspected incident, and what users might need to do to assist with incident handling. In addition, the organization should conduct awareness activities for IT staff involved in malware incident prevention and provide training on specific tasks.

## Organizations should have vulnerability mitigation capabilities to help prevent malware incidents.

Organizations should have documented policy, processes, and procedures to mitigate known vulnerabilities that malware might exploit. Because a vulnerability usually can be mitigated through one or more methods, organizations should use an appropriate combination of techniques, including security automation technologies with security configuration checklists and patch management, and additional host hardening measures so that effective techniques are readily available for various types of vulnerabilities.

## Organizations should have threat mitigation capabilities to assist in containing malware incidents.

Organizations should perform threat mitigation to detect and stop malware before it can affect its targets. The most commonly used malware threat mitigation technical control is antivirus software; organizations should deploy antivirus software on all hosts for which satisfactory antivirus software is available.

Additional technical controls that are helpful for malware threat mitigation include intrusion prevention systems, firewalls, content filtering and inspection, and application whitelisting. The System and Information Integrity family of security controls in NIST Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*, recommends having malware protection mechanisms on various types of hosts, including workstations, servers, mobile computing devices, firewalls, email servers, web servers, and remote access servers.

## Organizations should consider using defensive architecture methods to reduce the impact of malware incidents.

No matter how rigorous vulnerability and threat mitigation efforts are, malware incidents will still occur. Organizations should consider altering the defensive architecture of their hosts’ software to help mitigate those incidents that still occur. One technique is sandboxing, which is a security model where applications are run within a controlled environment that restricts what operations the applications can perform and isolates them from other applications. Another technique is browser separation, which involves using different web browsers for different types of website access (corporate applications, general access, etc.) Finally, segregation through virtualization techniques separate applications or operating systems from each other through the use of virtualization, such as having one OS instance for corporate applications and another OS instance for all other activity.

## Organizations should have a robust incident response process capability that addresses malware incident handling.

As *Computer Security Incident Handling Guide*, the incident response process has four main phases: preparation, detection and analysis, containment/eradication/recovery, and

post-incident activity. Some major recommendations for malware incident handling, by phase or subphase, are as follows:

* **Preparation.** Organizations should perform preparatory measures to ensure that they can respond effectively to malware incidents. Recommended actions include—
  + Building and maintaining malware-related skills within the incident response team
  + Facilitating communication and coordination throughout the organization
  + Acquiring the necessary tools (hardware and software) and resources to assist in malware incident handling
* **Detection and Analysis.** Organizations should strive to detect and validate malware incidents rapidly to minimize the number of infected hosts and the amount of damage the organization sustains. Recommended actions include—
  + Analyzing any suspected malware incident and validating that malware is the cause. This includes identifying characteristics of the malware activity by examining detection sources, such as antivirus software, intrusion prevention systems, and security information and event management (SIEM) technologies.
  + Identifying which hosts are infected by the malware, so that the hosts can undergo the appropriate containment, eradication, and recovery actions. Identifying infected hosts is often complicated by the dynamic nature of malware and computing. Organizations should carefully consider host identification issues before a large-scale malware incident occurs so that they are prepared to use multiple strategies for identifying infected hosts as part of their containment efforts. Organizations should select a sufficiently broad range of identification approaches and should develop procedures and technical capabilities to perform each selected approach effectively when a major malware incident occurs.
  + Prioritizing the handling of each incident based on NIST SP 800-61 guidelines and additional malware-specific criteria
  + Studying the behavior of malware by analyzing it either actively (executing the malware) or forensically (examining an infected host for evidence of malware)
* **Containment.** Malware incident containment has two major components: stopping the spread of malware and preventing further damage to hosts. Nearly every malware incident requires containment actions. In addressing an incident, it is important for an organization to decide which methods of containment to employ initially, early in the response. Organizations should have strategies and procedures in place for making containment-related decisions that reflect the level of risk acceptable to the organization. Containment strategies should support incident handlers in selecting the appropriate combination of containment methods based on the characteristics of a particular situation. Specific containment-related recommendations include the following:
  + It can be helpful to provide users with instructions on how to identify infections and what measures to take if a host is infected; however, organizations should not rely primarily on users for containing malware incidents.

If malware cannot be identified and contained by updated antivirus software, organizations should be prepared to use other security tools to contain it. Organizations should also be prepared to submit copies of unknown malware to their security software vendors for analysis, as well as contacting trusted parties such as incident response organizations and antivirus vendors when guidance is needed on handling new threats.

* + Organizations should be prepared to shut down or block services used by malware to contain an incident and should understand the consequences of doing so. Organizations should also be prepared to respond to problems caused by other organizations disabling their own services in response to a malware incident.
  + Organizations should be prepared to place additional temporary restrictions on network connectivity to contain a malware incident, such as suspending Internet access or physically disconnecting hosts from networks, recognizing the impact that the restrictions might have on organizational functions.
* **Eradication.** The primary goal of eradication is to remove malware from infected hosts. Because of the potential need for extensive eradication efforts, organizations should be prepared to use various combinations of eradication techniques simultaneously for different situations. Organizations should also consider performing awareness activities that set expectations for eradication and recovery efforts; these activities can be helpful in reducing the stress that major malware incidents can cause.
* **Recovery.** The two main aspects of recovery from malware incidents are restoring the functionality and data of infected hosts and removing temporary containment measures. Organizations should carefully consider possible worst-case scenarios and determine how recovery should be performed, including rebuilding compromised hosts from scratch or known good backups. Determining when to remove temporary containment measures, such as suspension of services or connectivity, is often a difficult decision during major malware incidents. Incident response teams should strive to keep containment measures in place until the estimated number of infected hosts and hosts vulnerable to infection is sufficiently low that subsequent incidents should be of little consequence. However, even though the incident response team should assess the risks of restoring services or connectivity, management ultimately should be responsible for determining what should be done based on the incident response team’s recommendations and management’s understanding of the business impact of maintaining the containment measures.
* **Post-Incident Activity.** Because the handling of malware incidents can be extremely expensive, it is particularly important for organizations to conduct a robust assessment of lessons learned after major malware incidents to prevent similar incidents from occurring. Capturing the lessons learned from the handling of such incidents should help an organization improve its incident handling capability and malware defenses, including identifying needed changes to security policy, software configurations, and malware detection and prevention software deployments.

# 2. Understanding Malware Threats

*Malware*, also known as *malicious code,* refers to a program that is covertly inserted into another program with the intent to destroy data, run destructive or intrusive programs, or otherwise compromise the confidentiality, integrity, or availability of the victim’s data, applications, or operating system. Malware is the most common external threat to most hosts, causing widespread damage and disruption and necessitating extensive recovery efforts within most organizations.

This section provides basic information on various forms of malware. It defines common terminology that is used throughout the rest of the document, and it presents fundamental concepts of malware. It does not attempt to explain how these different types of malware work in detail, but rather it highlights the basic characteristics of each type of malware. This section first discusses attacker tools, which are often delivered to targeted hosts via malware, and malware toolkits, which are used by attackers to construct malware. The rest of the section examines forms of malware: traditional, phishing, web-based malware, and advanced persistent threats.

## Forms of Malware

Malware has become the greatest external threat to most hosts, causing damage and requiring extensive recovery efforts within most organizations. The following are the classic categories of malware:

* + - **Viruses.** A virus self-replicates by inserting copies of itself into host programs or data files. Viruses are often triggered through user interaction, such as opening a file or running a program. Viruses can be divided into the following two subcategories:
      * **Compiled Viruses.** A compiled virus is executed by an operating system. Types of compiled viruses include file infector viruses, which attach themselves to executable programs; boot sector viruses, which infect the master boot records of hard drives or the boot sectors of removable media; and multipartite viruses, which combine the characteristics of file infector and boot sector viruses.
      * **Interpreted Viruses.** Interpreted viruses are executed by an application. Within this subcategory, macro viruses take advantage of the capabilities of applications’ macro programming language to infect application documents and document templates, while scripting viruses infect scripts that are understood by scripting languages processed by services on the OS.
    - **Worms.** A worm is a self-replicating, self-contained program that usually executes itself without user intervention. Worms are divided into two categories:
      * **Network Service Worms.** A network service worm takes advantage of a vulnerability in a network service to propagate itself and infect other hosts.
      * **Mass Mailing Worms.** A mass mailing worm is similar to an email-borne virus but is self- contained, rather than infecting an existing file.
    - **Trojan Horses.** A Trojan horse is a self-contained, nonreplicating program that, while appearing to be benign, actually has a hidden malicious purpose. Trojan horses either replace existing files with malicious versions or add new malicious files to hosts. They often deliver other attacker tools to hosts.

* + - **Malicious Mobile Code.** Malicious mobile code is software with malicious intent that is transmitted from a remote host to a local host and then executed on the local host, typically without the user’s explicit instruction. Popular languages for malicious mobile code include Java, ActiveX, JavaScript, and VBScript.
    - **Blended Attacks.** A blended attack uses multiple infection or transmission methods. For example, a blended attack could combine the propagation methods of viruses and worms.

Many, if not most, instances of malware today are blended attacks. Current malware also relies heavily on *social engineering*, which is a general term for attackers trying to trick people into revealing sensitive information or performing certain actions, such as downloading and executing files that appear to be benign but are actually malicious. Because so many instances of malware have a variety of malware characteristics, the classic malware categories listed above (virus, worm, etc.) are considerably less useful than they used to be for malware incident handling. At one time, there were largely different procedures for handling incidents of each malware category; now there is largely one set of procedures for handling all malware incidents, thus nullifying the primary need for having categories.

Another problem with the classic categories is that newer forms of malware do not neatly fit into them. For example, in the growing trend of *web-based malware*, also known as drive-by-download, a user’s web browsing is redirected to an infected website, often with little or no use of social engineering techniques. The infected website then attempts to exploit vulnerabilities on the user’s host and ultimately to install rootkits or other attacker tools onto the host, thus compromising the host. Although the website is infected, its malware does not infect the user’s host; rather, it functions as an attacker tool and installs other attacker tools on the host. Web-based malware is a blended attack of sorts, but its components do not map to the other malware categories.

The classic malware categories do not include *phishing*, which refers to use of deceptive computer-based means to trick individuals into disclosing sensitive personal information.[3](file:///C:\Users\pramoda.kumar\Downloads\NIST.SP.800-83r1.docx#_bookmark10) To perform a phishing attack, an attacker creates a website or email that looks as if it is from a well-known organization, such as an online business, credit card company, or financial institution. The fraudulent emails and websites are intended to deceive users into disclosing personal data, usually financial information. For example, phishers might seek usernames and passwords for online banking sites, as well as bank account numbers. Some phishing attacks overlap with web-based malware, because they install keystroke loggers or other attacker tools onto hosts to gather additional personal information.

Organizations should avoid expending substantial time and resources in categorizing each malware incident based on the types of categories expressed above.

## Attacker Tools

Various types of attacker tools might be delivered to a host by malware. These tools allow attackers to have unauthorized access to or use of infected hosts and their data, or to launch additional attacks. Popular types of attacker tools are as follows:

* + - **Backdoors.** A backdoor is a malicious program that listens for commands on a certain TCP or UDP port. Most backdoors allow an attacker to perform a certain set of actions on a host, such as acquiring passwords or executing arbitrary commands. Types of backdoors include zombies (better known as bots), which are installed on a host to cause it to attack other hosts, and remote

|  |
| --- |
|  |
|  | C:\Users\PRAMOD~1.KUM\AppData\Local\Temp\ksohtml16736\wps1.png |

administration tools, which are installed on a host to enable a remote attacker to gain access to the host’s functions and data as needed.

* + - **Keystroke Loggers.** A keystroke logger monitors and records keyboard use. Some require the attacker to retrieve the data from the host, whereas other loggers actively transfer the data to another host through email, file transfer, or other means.
    - **Rootkits.** A rootkit is a collection of files that is installed on a host to alter its standard functionality in a malicious and stealthy way. A rootkit typically makes many changes to a host to hide the rootkit’s existence, making it very difficult to determine that the rootkit is present and to identify what the rootkit has changed.
    - **Web Browser Plug-Ins.** A web browser plug-in provides a way for certain types of content to be displayed or executed through a web browser. Malicious web browser plug-ins can monitor all use of a browser.
    - **E-Mail Generators.** An email generating program can be used to create and send large quantities of email, such as malware and spam, to other hosts without the user’s permission or knowledge.
    - **Attacker Toolkits.** Many attackers use toolkits containing several different types of utilities and scripts that can be used to probe and attack hosts, such as packet sniffers, port scanners, vulnerability scanners, password crackers, and attack programs and scripts.

Because attacker tools can be detected by antivirus software, some people think of them as forms of malware. However, attacker tools have no infections capability on their own; they rely on malware or other attack mechanisms to install them onto target hosts. Strictly speaking, attacker tools are not malware, but because they are so closely tied to malware and often detected and removed using the same tools, attacker tools will be covered where appropriate throughout this publication.

## The Nature of Today’s Malware

The characteristic of today’s malware that most distinguishes it from previous generations of malware is its degree of customization. It has become trivial for attackers to create their own malware by acquiring malware toolkits, such as Zeus, SpyEye, and Poison Ivy, and customizing the malware produced by those toolkits to meet their individual needs. Many of these toolkits are available for purchase, while others are open source, and most have user-friendly interfaces that make it simple for unskilled attackers to create customized, high-capability malware.

# 3. Malware Incident Prevention

This section presents recommendations for preventing malware incidents within an organization. The main elements of prevention are policy, awareness, vulnerability mitigation, threat mitigation, and defensive architecture. Ensuring that policies address malware prevention provides a basis for implementing preventive controls. Establishing and maintaining general malware awareness programs for all users, as well as specific awareness training for the IT staff directly involved in malware prevention– related activities, are critical to reducing the number of incidents that occur through human error.

Expending effort on vulnerability mitigation can eliminate some possible attack vectors. Implementing a combination of threat mitigation techniques and tools, such as antivirus software and firewalls, can prevent threats from successfully attacking hosts and networks. Also, using defensive architectures such as sandboxing, browser separation, and segregation through virtualization can reduce the impact of compromises. Sections 3.1 through 3.5 address each of these areas in detail and explain that organizations should implement guidance from each category of recommendations to create an effective layered defense against malware.

When planning an approach to malware prevention, organizations should be mindful of the attack vectors that are most likely to be used currently and in the near future.[4](file:///C:\Users\pramoda.kumar\Downloads\NIST.SP.800-83r1.docx#_bookmark14) They should also consider how well- controlled their hosts are (e.g., managed environment, non-managed environment); this has significant bearing on the effectiveness of various preventive approaches. In addition, organizations should incorporate existing capabilities, such as antivirus software deployments and patch management programs, into their malware prevention efforts. However, organizations should be aware that no matter how much effort they put into malware incident prevention, incidents will still occur (e.g., previously unknown types of threats, human error). For this reason, as described in Section 4, organizations should have robust malware incident handling capabilities to limit the damage that malware can cause and restore data and services efficiently.

## Policy

Organizations should ensure that their policies address prevention of malware incidents. These policy statements should be used as the basis for additional malware prevention efforts, such as user and IT staff awareness, vulnerability mitigation, threat mitigation, and defensive architecture (described in Sections

* 1. through 3.5, respectively). If an organization does not state malware prevention considerations clearly in its policies, it is unlikely to perform malware prevention activities consistently and effectively throughout the organization. Malware prevention–related policy should be as general as possible to provide flexibility in policy implementation and to reduce the need for frequent policy updates, but also specific enough to make the intent and scope of the policy clear. Although some organizations have separate malware policies, many malware prevention considerations belong in other policies, such as acceptable use policies, so a separate malware policy might duplicate some of the content of other policies.[5](file:///C:\Users\pramoda.kumar\Downloads\NIST.SP.800-83r1.docx#_bookmark15) Malware prevention–related policy should include provisions related to remote workers—both those using hosts controlled by the organization and those using hosts outside of the organization’s control (e.g., contractor computers, employees’ home computers, business partners’ computers, mobile devices).

Common malware prevention–related policy considerations include the following:[6](file:///C:\Users\pramoda.kumar\Downloads\NIST.SP.800-83r1.docx#_bookmark17)

* + - Requiring the scanning of media from outside of the organization for malware before they can be used
    - Requiring that email file attachments be scanned before they are opened
    - Prohibiting the sending or receipt of certain types of files (e.g., .exe files) via email
    - Restricting or prohibiting the use of unnecessary software, such as user applications that are often used to transfer malware (e.g., personal use of external instant messaging and file sharing services)
    - Restricting the use of removable media (e.g., flash drives), particularly on hosts that are at high risk of infection, such as publicly accessible kiosks
    - Specifying which types of preventive software (e.g., antivirus software, content filtering software) are required for each type of host (e.g., email server, web server, laptop, smart phone) and application (e.g., email client, web browser), and listing the high-level requirements for configuring and maintaining the software (e.g., software update frequency, host scan scope and frequency)
    - Restricting or prohibiting the use of organization-issued and/or personally-owned mobile devices on the organization’s networks and for telework/remote access.

## Awareness

An effective awareness program explains proper rules of behavior for use of an organization’s IT hosts and information. Accordingly, awareness programs should include guidance to users on malware incident prevention, which can help reduce the frequency and severity of malware incidents. All users should be made aware of the ways in which malware enters and infects hosts; the risks that malware poses; the inability of technical controls to prevent all incidents; and the importance of users in preventing incidents, with an emphasis on avoiding social engineering attacks (as discussed below). In addition, the organization’s awareness program should cover the malware incident prevention considerations in the organization’s policies and procedures, as described in Section 3.1, as well as generally recommended practices for avoiding malware incidents. Examples of such practices are as follows:

* + - Not opening suspicious emails or email attachments, clicking on hyperlinks, etc. from unknown or known senders, or visiting websites that are likely to contain malicious content
    - Not clicking on suspicious web browser popup windows
    - Not opening files with file extensions that are likely to be associated with malware (e.g., .bat,

.com, .exe, .pif, .vbs)

* + - Not disabling malware security control mechanisms (e.g., antivirus software, content filtering software, reputation software, personal firewall)
    - Not using administrator-level accounts for regular host operation
    - Not downloading or executing applications from untrusted sources.