Malware is intrusive software that is designed to damage and destroy computers and computer systems. Malware is a contraction for “malicious software.” Examples of common malware includes viruses, worms, Trojan viruses, spyware, adware, and ransomware.

How do I protect my network against malware?

Typically, businesses focus on preventative tools to stop breaches. By securing the perimeter, businesses assume they are safe. Some advanced malware, however, will eventually make their way into your network. As a result, it is crucial to deploy technologies that continually monitor and detect malware that has evaded perimeter defenses. Sufficient advanced [malware protection](https://www.cisco.com/c/en_in/products/security/advanced-malware-protection/index.html) requires multiple layers of safeguards along with high-level network visibility and intelligence.

How do I detect and respond to malware?

Malware will inevitably penetrate your network. You must have defenses that provide significant visibility and breach detection. In order to remove malware, you must be able to identify malicious actors quickly. This requires constant network scanning. Once the threat is identified, you must remove the malware from your network. Today's antivirus products are not enough to protect against advanced cyber threats. Learn how to [update your antivirus strategy](https://www.cisco.com/c/en/us/products/security/amp-for-endpoints/best-antivirus-strategy.html).

Types of malware

Virus

Viruses are a subgroup of malware. A virus is malicious software attached to a document or file that supports macros to execute its code and spread from host to host. Once downloaded, the virus will lay dormant until the file is opened and in use. Viruses are designed to disrupt a system’s ability to operate. As a result, viruses can cause significant operational issues and data loss.

Worms

Worms are a malicious software that rapidly replicates and spreads to any device within the network. Unlike viruses, worms do not need host programs to disseminate. A worm infects a device via a downloaded file or a network connection before it multiplies and disperses at an exponential rate. Like viruses, worms can severely disrupt the operations of a device and cause data loss.

Trojan virus

Trojan viruses are disguised as helpful software programs. But once the user downloads it, the Trojan virus can gain access to sensitive data and then modify, block, or delete the data. This can be extremely harmful to the performance of the device. Unlike normal viruses and worms, Trojan viruses are not designed to self-replicate.

Spyware

Spyware is malicious software that runs secretly on a computer and reports back to a remote user. Rather than simply disrupting a device’s operations, spyware targets sensitive information and can grant remote access to predators. Spyware is often used to steal financial or personal information. A specific type of spyware is a keylogger, which records your keystrokes to reveal passwords and personal information.

Adware

Adware is malicious software used to collect data on your computer usage and provide appropriate advertisements to you. While adware is not always dangerous, in some cases adware can cause issues for your system. Adware can redirect your browser to unsafe sites, and it can even contain Trojan horses and spyware. Additionally, significant levels of adware can slow down your system noticeably. Because not all adware is malicious, it is important to have protection that constantly and intelligently scans these programs.

Ransomware

Ransomware is malicious software that gains access to sensitive information within a system, encrypts that information so that the user cannot access it, and then demands a financial payout for the data to be released. Ransomware is commonly part of a phishing scam. By clicking a disguised link, the user downloads the ransomware. The attacker proceeds to encrypt specific information that can only be opened by a mathematical key they know. When the attacker receives payment, the data is unlocked.

Fileless malware

[Fileless malware](https://blogs.cisco.com/security/in-pursuit-of-invisibility-fileless-malware) is a type of memory-resident malware. As the term suggests, it is malware that operates from a victim’s computer’s memory, not from files on the hard drive. Because there are no files to scan, it is harder to detect than traditional malware. It also makes forensics more difficult because the malware disappears when the victim computer is rebooted. In late 2017, the Cisco Talos threat intelligence team posted an example of fileless malware that they called DNSMessenger.

# **Viruses and Similar Threats**

Viruses, worms, Trojan horses and related computer threats are commonly confused with each other because they often cause similar damage. Viruses have been around longer than the others, and consequently the term “virus” is commonly but inaccurately used to refer to all of them. Here are some distinguishing characteristics:

**Virus**  
A virus is a relatively small file that can copy itself into another file or program (its host). It can be transmitted only if its host file or program is transmitted. Some viruses are designed to change themselves slightly in order to make their detection and removal more difficult. Many viruses are merely annoyances, but some can be very destructive. As a whole, they are less common now than in the past. For more information, see the Wikipedia page on [Computer virus](https://en.wikipedia.org/wiki/Computer_virus).

**Trojan horse**  
A Trojan horse is a program that appears to be useful or entertaining, but it carries a hidden malicious function that is activated when the program is run. Some Trojan horses even masquerade as repair tools, claiming to remove threats from your computer but actually doing the opposite. Older Trojan horses could not transmit themselves, but more recent versions can. This blurs the traditional distinction between viruses and Trojan horses. For more information, see the Wikipedia page on [Trojan horse (computing)](https://en.wikipedia.org/wiki/Trojan_horse_%28computing%29)

**Worm**  
A worm is a program that can both copy and transmit itself. This type of threat is now more common and often more disruptive than many viruses. For more information, see the Wikipedia page on [Computer worm](https://en.wikipedia.org/wiki/Computer_worm).

**Malicious script**These vary in the harm they can cause, and they can get into your computer or compromise your personal information by a number of means; e.g., when you click on a link inside an specially designed fradulent email or submit a form that has such a script hidden inside it.

**How they spread and what they do**Electronic threats are usually spread by opening infected email attachments and by downloading infected files. Clicking on links inside certain emails can result in threats being downloaded to your machine. They can even enter your computer as attachments to Instant Messages. When these threats are being transmitted in large numbers, they can significantly drain network resources and slow down Internet traffic. When one of them infects your computer, it might take one or more of the following actions:

* Operate silently, with no obvious indication of its presence
* Remain dormant initially and activate later at a specified time or when you perform a certain action
* Destroy or corrupt your files
* Send copies of itself to all of your email contacts, potentially infecting them as well
* Deactivate your antivirus software
* Prevent you from using your browser to download virus removal tools
* Log your keystrokes and steal credit card numbers and passwords when you make purchases or bank online.
* Hijack your browser and take you to Web sites where you may be fooled into entering personal information such as account passwords
* Hijack your computer and use it maliciously or commercially, making you appear to be the perpetrator.

**What you can do about them**  
While it is useful to understand the technical distinctions among these threats and important to know what damage they can cause, it is crucial that you maximize your protection against them and minimize their spread to other computer users. It is particularly important to **keep the following items updated** every few days or as often as the software recommends. You can set many of these programs to have the updating done automatically.

* Operating system
* Web browsers
* Instant Message software
* Microsoft Office and other applications with known vulnerabilities
* Antivirus definitions
* Antispyware