Malware

Malware, short for malicious software, is a blanket term for viruses, worms, trojans and other harmful computer programs hackers use to wreak destruction and gain access to sensitive information.

Malware is a catch-all term to refer to any software designed to cause damage to a single computer, server, or computer network." In other words, software is identified as malware based on its intended use, rather than a particular technique or technology used to build it.

This means that the question of, say, what the difference is between malware and a virus misses the point a bit: **a virus is a type of malware, so all viruses are malware (but not every piece of malware is a virus)**.

Types of malware

There are a number of different ways of categorizing malware; t**he first is by how the malicious software spreads.**

- A **worm** is a standalone piece of malicious software that reproduces itself and spreads from computer to computer.
- A **virus** is a piece of computer code that inserts itself within the code of another standalone program, then forces that program to take malicious action and spread itself.
- A **trojan** is a program that cannot reproduce itself but masquerades as something the user wants and tricks them into activating it so it can do its damage and spread.

Another way to categorize malware is by what it does once it has successfully infected its victim's computers. There are a wide range of potential attack techniques used by malware:

- **Spyware** is defined as **"malware used for the purpose of secretly gathering data on an unsuspecting user."** In essence, it spies on your behavior as you use your computer, and on the data you send and receive, usually with the purpose of sending that information to a third party. A keylogger is a specific kind of spyware that records all the keystrokes a user makes—great for stealing passwords.
- A **rootkit** is, described as **"a program or, more often, a collection of software tools that gives a threat actor remote access to and control over a computer or other system."** It gets its name because it's a kit of tools that (generally illicitly) gain root access (administrator-level control, in Unix terms) over the target system, and use that power to hide their presence.
- **Adware** is malware that forces your browser to redirect to web advertisements, which often themselves seek to download further, even more malicious software. Adware often piggybacks onto tempting **"free"** programs like games or browser extensions.
- **Ransomware** is a flavor of malware that encrypts your hard drive's files and demands a payment, usually in Bitcoin, in exchange for the decryption key. Several high-profile malware outbreaks of the last few years, such as **WannaCry**, are ransomware. Without the decryption key, it's mathematically

impossible for victims to regain access to their files. So-called **scareware** is a sort of shadow version of ransomware; it claims to have taken control of your computer and demands a ransom, but actually is just using tricks like browser redirect loops to make it seem as if it's done more damage than it really has, and unlike ransomware can be relatively easily disabled.

- **Cryptojacking** is another way attackers can force you to supply them with Bitcoin—only it works without you necessarily knowing. The crypto mining malware infects your computer and uses your CPU cycles to mine Bitcoin for your attacker's profit. The mining software may run in the background on your operating system or even as JavaScript in a browser window.
- **Malvertising** is the use of legitimate ads or ad networks to covertly deliver malware to unsuspecting users' computers. For example, a cyber criminal might pay to place an ad on a legitimate website. When a user clicks on the ad, code in the ad either redirects them to a malicious website or installs malware on their computer. In some cases, the malware embedded in an ad might execute automatically without any action from the user, a technique referred to as a **"drive-by download."**

VIRUSES

How does a computer virus attack?

Once a virus has successfully attached to a program, file, or document, the virus will lie dormant until circumstances cause the computer or device to execute its code. In order for a virus to infect your computer, you have to run the infected program, which in turn causes the virus code to be executed.

This means that a virus can remain dormant on your computer, without showing major signs or symptoms. However, once the virus infects your computer, the virus can infect other computers on the same network. Stealing passwords or data, logging keystrokes, corrupting files, spamming your email contacts, and even taking over your machine are just some of the devastating and irritating things a virus can do.

While some viruses can be playful in intent and effect, others can have profound and damaging effects. This includes erasing data or causing permanent damage to your hard disk. Worse yet, some viruses are designed with financial gains in mind.

How do computer viruses spread?

In a constantly connected world, you can contract a computer virus in many ways, some more obvious than others. Viruses can be spread through email and text message attachments, Internet file downloads, and social media scam links. Your mobile devices and smartphones can become infected with mobile viruses through shady app downloads. Viruses can hide disguised as attachments of socially shareable content such as funny images, greeting cards, or audio and video files.

To avoid contact with a virus, it's important to exercise caution when surfing the web, downloading files, and opening links or attachments. To help stay safe, never download text or email attachments that you're not expecting, or files from websites you don't trust.

What are the different types of computer viruses?

1. Boot sector virus
This type of virus can take control when you start — or boot — your computer. One way it can spread is by plugging an infected USB drive into your computer.

2. Web scripting virus
This type of virus exploits the code of web browsers and web pages. If you access such a web page, the virus can infect your computer.

3. Browser hijacker
This type of virus “hijacks” certain web browser functions, and you may be automatically directed to an unintended website.

4. Resident virus
This is a general term for any virus that inserts itself in a computer system’s memory. A resident virus can execute anytime when an operating system loads.

5. Direct action virus
This type of virus comes into action when you execute a file containing a virus. Otherwise, it remains dormant.

6. Polymorphic virus
A polymorphic virus changes its code each time an infected file is executed. It does this to evade antivirus programs.

7. File infector virus
This common virus inserts malicious code into executable files — files used to perform certain functions or operations on a system.

8. Multipartite virus
This kind of virus infects and spreads in multiple ways. It can infect both program files and system sectors.

9. Macro virus
Macro viruses are written in the same macro language used for software applications. Such viruses spread when you open an infected document, often through email attachments.

WORMS

How does a computer worm attack?

A computer worm is a type of malware that spreads copies of itself from computer to computer. A worm can replicate itself without any human interaction, and it does not need to attach itself to a software program in order to cause damage.

How do computer worms work?

Worms can be transmitted via software vulnerabilities or computer worms could arrive as attachments in spam emails or instant messages (IMs). Once opened, these files could provide a link to a malicious website or automatically download the computer worm. Once it’s installed, the worm silently goes to work and infects the machine without the user’s knowledge.

Worms can modify and delete files, and they can even inject additional malicious software onto a computer. Sometimes a computer worm’s purpose is only to make copies of itself over and over — depleting system resources, such as hard drive space or bandwidth, by overloading a shared network. In addition to wreaking havoc on a computer’s resources, worms can also steal data, install a backdoor, and allow a hacker to gain control over a computer and its system settings.

How to tell if your computer has a worm

If you suspect your devices are infected with a computer worm, run a virus scan immediately. Even if the scan comes up negative, continue to be proactive by following these steps.

- **Keep an eye on your hard drive space**. When worms repeatedly replicate themselves, they start to use up the free space on your computer.
- **Monitor speed and performance.** Has your computer seemed a little sluggish lately? Are some of your programs crashing or not running properly? That could be a red flag that a worm is eating up your processing power.
- **Be on the lookout for missing or new files**. One function of a computer worm is to delete and replace files on a computer.

How to help protect against computer worms

Computer worms are just one example of malicious software. To help protect your computer from worms and other online threats, take these steps.

- Since software vulnerabilities are major infection vectors for computer worms, be sure your computer’s operating system and applications are up to date with the latest versions. Install these updates as soon as they’re available because updates often include patches for security flaws.
- Phishing is another popular way for hackers to spread worms (and other types of malware). Always be extra cautious when opening unsolicited emails, especially those from unknown senders that contain attachments or dubious links.
- Be sure to invest in a strong internet security software solution that can help block these threats. A good product should have anti-phishing technology as well as defenses against viruses, spyware, ransomware, and other online threats.

TROJANS

What is a Trojan Horse ?

A Trojan horse, or Trojan, is a type of malicious code or software that looks legitimate but can take control of your computer. A Trojan is designed to damage, disrupt, steal, or in general inflict some other harmful action on your data or network.

A Trojan acts like a bona fide application or file to trick you. It seeks to deceive you into loading and executing the malware on your device. Once installed, a Trojan can perform the action it was designed for.

A Trojan is sometimes called a Trojan virus or a Trojan horse virus, but that's a misnomer. Viruses can execute and replicate themselves. A Trojan cannot. A user has to execute Trojans. Even so, Trojan malware and Trojan virus are often used interchangeably.

How do Trojans work?

Here's a Trojan malware example to show how it works.

You might think you've received an email from someone you know and click on what looks like a legitimate attachment. But you've been fooled. The email is from a cybercriminal, and the file you clicked on — and downloaded and opened — has gone on to install malware on your device.

When you execute the program, the malware can spread to other files and damage your computer.

How? It varies. Trojans are designed to do different things. But you'll probably wish they weren't doing any of them on your device.

Common types of Trojan malware, from A to Z

Here's a look at some of the most common types of Trojan malware, including their names and what they do on your computer:

Backdoor Trojan

This Trojan can create a "backdoor" on your computer. It lets an attacker access your computer and control it. Your data can be downloaded by a third party and stolen. Or more malware can be uploaded to your device.

Distributed Denial of Service (DDoS) attack Trojan

This Trojan performs DDoS attacks. The idea is to take down a network by flooding it with traffic. That traffic comes from your infected computer and others.

Downloader Trojan

This Trojan targets your already-infected computer. It downloads and installs new versions of malicious programs. These can include Trojans and adware.

Fake AV Trojan

This Trojan behaves like antivirus software, but demands money from you to detect and remove threats, whether they’re real or fake.

Game-thief Trojan

The losers here may be online gamers. This Trojan seeks to steal their account information.

Infostealer Trojan

As it sounds, this Trojan is after data on your infected computer.

Mailfinder Trojan

This Trojan seeks to steal the email addresses you’ve accumulated on your device.

Ransom Trojan

This Trojan seeks a ransom to undo damage it has done to your computer. This can include blocking your data or impairing your computer’s performance.

Remote Access Trojan

This Trojan can give an attacker full control over your computer via a remote network connection. Its uses include stealing your information or spying on you.

Rootkit Trojan

A rootkit aims to hide or obscure an object on your infected computer. The idea? To extend the time a malicious program runs on your device.

SMS Trojan

This type of Trojan infects your mobile device and can send and intercept text messages. Texts to premium-rate numbers can drive up your phone costs.

Trojan banker

This Trojan takes aim at your financial accounts. It’s designed to steal your account information for all the things you do online. That includes banking, credit card, and bill pay data.

Trojan IM

This Trojan targets instant messaging. It steals your logins and passwords on IM platforms.

That’s just a sample. There are a lot more.