Malware

Malware is any type of software created to harm or exploit another piece of software or hardware. Short for “malicious software,” malware is a collective term used to describe viruses, ransomware, spyware, Trojans, and any other type of code or software built with malicious intent.

# HOw does it work?

For malware to work, it usually needs you to do something first to get the software on your computer. That means clicking a link, opening an attachment, or visiting an infected website. Once on your machine, the malware’s payload begins the task it’s designed to perform — stealing your data, encrypting your files, installing additional malware, and so on.

Malware will stay on your system until it’s been detected and removed. And some malicious software will try to block or hide from any antivirus apps or other security tools you may have.

# Types

## Virus

Computer viruses infect clean files and spread to other clean files. They can spread uncontrollably, damaging a system’s core functionality and deleting or corrupting files.

**Macro viruses**

Exploit macros in Microsoft Office apps like Word and Excel to infect your device.

**Router viruses**

Your Wi-Fi router can also become infected with malware. Router malware usually redirects you to malicious pharming websites that can capture your personal data, and removing router viruses can be tricky.

## Trojans

Disguised as legitimate software or are hidden in legitimate software that’s been tampered with. A Trojan’s job is to sneak onto your device and install additional malware.

## Spyware

Malware designed to spy on you. It hides in the background and collects your data, including passwords, GPS location, and financial information. Fortunately, removing spyware from your Mac or PC usually isn’t very difficult.

Keyloggers

Type of spyware that hide on your device while recording all your keystrokes. They can capture login credentials, credit card numbers, and more.

## Worms

Worms are a bit different from viruses, because they can spread without a host file. Worms infect entire networks of devices, using each consecutively infected machine to infect others.

## Ransomware

Ransomware locks up your computer and your files, and threatens to erase everything unless you pay a ransom. It’s one of today’s most pressing malware threats.

## Adware

Adware is malicious software that spams you with ads to generate revenue for the attacker. Adware undermines your security to serve you ads — which can give other malware an easy way in.

## Scareware

Scareware uses social engineering tricks to frighten you into installing it. A fake pop-up warns you that your computer is infected with a virus, and the solution will be to download a scam “security” program.

## Botnets

Botnets aren’t technically malware — they’re networks of infected computers that work together under the control of an attacker. Botnets are often used to commit DDoS attacks.

## Rootkits

Rootkits are a dangerous, hard-to-detect form of malware that burrow deep into your computer to give a hacker full administrative access. The best way to deal with them is by using a dedicated rootkit removal tool.

## Browser hijackers

Browser hijackers are malware that modify your web browser without your consent, and often without your knowledge. They may redirect you to harmful websites or spam you with extra ads. Removing browser hijackers usually is quite simple, but it’s always good to use secure and private browsers.

## Cryptominers

Cryptominer malware is malicious software that hijacks a victim’s computer’s processing power to mine cryptocurrency for the attacker in a practice known as cryptojacking. Many cryptominers use browser hijacking to take over computers.

## Logic bombs

Logic bombs are bits of malicious code designed to execute after a specified condition has been met. Time bombs are a subset of logic bombs that lie dormant until a certain time or date.

# Signs of malware

**Sudden performance drops**: Malware can occupy a lot of your device’s processing power, resulting in severe slowdowns. That’s why removing malware is one way to speed up your PC.

**Frequent crashes and freezing**: Some malware will cause your computer to freeze or crash, while other types will cause crashes by consuming too much RAM or driving up CPU temperatures. Sustained high CPU usage may be a sign of malware.

**Deleted or corrupted files**: Malware often deletes or corrupts files as part of its plan to cause as much chaos as possible.

Lots of **pop-up ads**: Adware’s job is to spam you with pop-ups. Other types of malware may cause pop-up ads and alerts as well.

**Browser redirects**: If your browser keeps sending you to sites that you aren’t trying to visit, a malware attack may have made changes to your DNS settings.

Your **contacts are receiving strange messages** from you: Some malware spreads by emailing or messaging victims’ contacts. Secure messaging apps can help protect your communications from eavesdroppers.

You see a **ransom note**: Ransomware wants you to know it’s there — it’ll take over your screen with a ransom note demanding payment to get your files back. A ransom note is an easy way to tell what malware is on your computer: it’s ransomware.

**Unfamiliar apps**: Malware can install additional apps on your device. If you see new programs that you didn’t install yourself, it may be the result of a malware attack.

# Why is malware used

**Data theft:** Dangerous cybercriminals can steal data and use it to commit identity theft or sell it on the dark web to other cybercriminals. Malware-based data theft can involve redirecting people to pharming websites, capturing passwords with spyware, and even large-scale data breaches.

**Corporate espionage:** Data theft on a corporate scale is known as corporate espionage. Companies can steal secrets from their competitors, and governments often target large corporations as well.

**Cyberwarfare and international espionage:** Governments around the world are frequently accused of using malware against other countries and large corporations.

**Sabotage:** Sometimes, damage is the goal. Attackers can delete files, wipe records, or shut down entire organizations to cause millions of dollars of damage.

**Extortion:** Ransomware encrypts a victim’s files or device and demands payment for the decryption key. The purpose is to get the victim — a person, institution, or government — to pay the ransom.

**Law enforcement:** Police and other government authorities can use spyware to monitor suspects and harvest information to use in their investigations.

**Entrepreneurship:** Many potent strains of ransomware are available to anyone as ransomware-as-a-service (RaaS), where the developer licenses their malware in exchange for an up-front fee or a cut of every payment.

**DDoS attacks:** Hackers can use malicious software to create botnets — linked networks of “zombie computers” under the attacker’s control. The botnet is then used to overload a server in a distributed denial of service (DDoS) attack.

**Mining cryptocurrency:** Cryptominers force a victim’s computer to generate, or mine, bitcoin or other cryptocurrency for the attacker.

# Types of malware attacks

**Email:** If your email has been hacked, malware can force your computer to send emails with infected attachments or links to malicious websites. When a recipient opens the attachment or clicks the link, the malware is installed on their computer, and the cycle repeats. Not opening attachments from unknown senders is an important part of good email security.

**Messaging apps:** Malware can spread by hijacking messaging apps to send infected attachments or malicious links to a victim’s contacts.

**Infected ads:** Hackers can load malware into ads and seed those ads on popular websites — a practice known as malvertising. When you click the infected ad, it downloads malware to your computer.

**Pop-up alerts:** Scareware uses fake security alerts to trick you into downloading bogus security software, which in some cases can be additional malware.

**Drive-by downloads:** A drive-by download happens when a malicious website automatically downloads malware onto your device. This happens as soon as you load the page — no clicks required. Hackers use DNS hijacking to automatically redirect you to these malicious sites.

**Personal installation:** People sometimes install parental control software on their partner’s computer or phone. When these apps are used without the victim’s consent, they become spyware.

**Physical media:** Hackers can load malware onto USB flash drives and wait for unsuspecting victims to plug them into their computers. This technique is often used in corporate espionage.

**Exploits:** Exploits are bits of code designed to take advantage of a vulnerability, or security weakness, in a piece of software or hardware. A blended threat is a specialized type of exploit package that targets multiple vulnerabilities at once.

# sources

<https://www.avg.com/en/signal/what-is-malware#:~:text=Malware%20is%20any%20type%20of,software%20built%20with%20malicious%20intent>.

<https://www.paloaltonetworks.com/cyberpedia/what-is-malware-protection>