What are the different types of malware?

What does malware mean?

The word ‘malware’ is a contraction of ‘malicious software’. Malware is intrusive software that is intentionally designed to cause damage to computers and computer systems. By contrast, software that causes unintentional damage is usually referred to as a software bug.

People sometimes ask about the difference between a virus and malware. The difference is that malware is an umbrella term for a range of online threats, including viruses, spyware, adware, ransomware, and other types of harmful software. A computer virus is simply one type of malware.

Malware may be introduced to a network through phishing, malicious attachments, malicious downloads, social engineering, or flash drives. In this overview, we look at common malware types.

Types of malware

It’s important to understand the different types of malware attacks to help protect yourself from being compromised. While some malware categories are well-known (at least by name), others are less so:

Adware

Adware, a contraction of ‘advertising-supported software’, displays unwanted and sometimes malicious advertising on a computer screen or mobile device, redirects search results to advertising websites, and captures user data that can be sold to advertisers without the user's consent. Not all adware is malware, some is legitimate and safe to use.

Users can often affect the frequency of adware or what kinds of downloads they allow by managing the pop-up controls and preferences within their internet browsers or using an ad blocker.

Adware examples:

- **Fireball** – Fireball hit the headlines in 2017 when an Israeli software company discovered that 250 million computers and one-fifth of the corporate networks worldwide were infected with it. When Fireball affects your computer, it takes over your browser. It changes your homepage to a fake search engine – Trotus – and inserts obtrusive ads into any webpage you visit. It also prevents you from modifying your browser settings.
- **Appearch** – Appearch is another common adware program that acts as a browser hijacker. Usually bundled with other free software, it inserts so many ads into the browser that web browsing becomes very difficult. When you attempt to visit a website, you're taken to Appearch.info instead. If you manage to open a web page, Appearch converts random blocks of text into links, so when you select the text, a pop-up invites you to download software updates.

Spyware

Spyware is a form of malware that hides on your device, monitors activity, and steals sensitive information like financial data, account information, logins, and more. Spyware can spread by exploiting software vulnerabilities or else be bundled with legitimate software or in Trojans.

Spyware examples:

- **CoolWebSearch** – This program took advantage of the security vulnerabilities in Internet Explorer to hijack the browser, change the settings, and send browsing data to its author.
- **Gator** – Usually bundled with file-sharing software like Kazaa, this program monitors the victim’s web surfing habits and uses the information to serve them with specific ads.

Ransomware and crypto-malware

Ransomware is malware designed to lock users out of their system or deny access to data until a ransom is paid. Crypto-malware is a type of ransomware that encrypts user files and requires payment by a specific deadline and often through a digital currency such as Bitcoin. Ransomware has been a persistent threat for organizations across industries for many years now. As more businesses embrace digital transformation, the likelihood of being targeted in a ransomware attack has grown considerably.

Ransomware examples:

- **CryptoLocker** is a form of malware prevalent in 2013 and 2014 which cyber criminals used to gain access to and encrypt files on a system. Cybercriminals used social engineering tactics to trick employees into downloading the ransomware onto their computers, infecting the network. Once downloaded, CryptoLocker would display a ransom message offering to decrypt the data if a cash or Bitcoin payment was made by the stated deadline. While the CryptoLocker ransomware has since been taken down, it is believed that its operators extorted around three million dollars from unsuspecting organizations.
- **Phobos malware** – a form of ransomware that appeared in 2019. This strain of ransomware is based on the previously known Dharma (aka CrySis) family of ransomware.

Trojans

A Trojan (or Trojan Horse) disguises itself as legitimate software to trick you into executing malicious software on your computer. Because it looks trustworthy, users download it, inadvertently allowing malware onto their device. Trojans themselves are a doorway. Unlike a worm, they need a host to work. Once a Trojan is installed on a device, hackers can use it to delete, modify or capture data, harvest your device as part of a botnet, spy on your device, or gain access to your network.

Trojan examples:

- **Qbot malware**, also known as 'Qakbot' or 'Pinkslipbot', is a banking Trojan active since 2007 focused on stealing user data and banking credentials. The malware has evolved to include new delivery mechanisms, command and control techniques, and anti-analysis features.
- **TrickBot malware** —first identified in 2016—is a Trojan developed and operated by sophisticated cybercrime actors. Originally designed as a banking Trojan to steal financial data, TrickBot has evolved into modular, multi-stage malware that provides its operators with a full suite of tools to carry out numerous illegal cyber activities.

Worms

One of the most common types of malware, worms, spread over computer networks by exploiting operating system vulnerabilities. A worm is a standalone program that replicates itself to infect other computers without requiring action from anyone. Since they can spread fast, worms are often used to execute a payload—a piece of code created to damage a system. Payloads can delete files on a host system, encrypt data for a ransomware attack, steal information, delete files, and create botnets.

Worm example:

- **SQL Slammer** was a well-known computer worm that did not use traditional distribution methods. Instead, it generated random IP addresses and sent itself out to them, looking for those not protected by antivirus software. Soon after it hit in 2003, the result was more than 75,000 infected computers unknowingly involved in DDoS attacks on several major websites. Though the relevant security patch has been available for many years now, SQL Slammer nevertheless experienced a resurgence in 2016 and 2017.

Viruses

A virus is a piece of code that inserts itself into an application and executes when the app is run. Once inside a network, a virus may be used to steal sensitive data, launch DDoS attacks, or conduct ransomware attacks. Usually spread via

infected websites, file sharing, or email attachment downloads, a virus will lie dormant until the infected host file or program is activated. Once that happens, the virus can replicate itself and spread through your systems.

Virus example:

- **Stuxnet** – Stuxnet appeared in 2010 and was widely believed to have been developed by the US and Israeli governments to disrupt Iran's nuclear program. Spread via a USB thumb drive, it targeted Siemens industrial control systems, causing centrifuges to fail and self-destroy at a record rate. It's believed that Stuxnet infected over 20,000 computers and ruined one-fifth of Iran's nuclear centrifuges – setting its program back years.

Keyloggers

A keylogger is a type of spyware that monitors user activity. Keyloggers can be used for legitimate purposes – for example, families who use them to keep track of their children's online activity or organizations which use them to monitor employee activity. However, when installed for malicious purposes, keyloggers can be used to steal password data, banking information, and other sensitive information. Keyloggers can be inserted into a system through phishing, social engineering, or malicious downloads.

Keylogger example:

- In 2017, a University of Iowa student was arrested after installing keyloggers on staff computers to steal login credentials to modify and change grades. The student was found guilty and sentenced to four months in prison.

Bots and botnets

A bot is a computer that has been infected with malware so it can be controlled remotely by a hacker. The bot – sometimes called a zombie computer – can then be used to launch more attacks or become part of a collection of bots called a botnet. Botnets can include millions of devices as they spread undetected. Botnets help hackers with numerous malicious activities, including DDoS attacks, sending spam and phishing messages, and spreading other types of malware.

Botnet examples:

- **Andromeda malware –** The Andromeda botnet was associated with 80 different malware families. It grew so large that it was at one point infecting a million new machines a month, distributing itself via social media, instant messaging, spam emails, exploit kits, and more. The operation was taken down by the FBI, Europol's European Cybercrime centre, and others in 2017 – but many PCs continued to be infected.

- **Mirai –** In 2016, a massive DDoS attack left much of the US East Coast without internet access. The attack, which authorities initially feared was the work of a hostile nation-state, was caused by the Mirai botnet. Mirai is a type of malware that automatically finds Internet of Things (IoT) devices to infect and conscripts them into a botnet. From there, this IoT army can be used to mount DDoS attacks in which a firehose of junk traffic floods a target's servers with malicious traffic. Mirai continues to cause trouble today.

PUP malware

PUPs – which stands for 'potentially unwanted programs' – are programs that may include advertising, toolbars, and pop-ups that are unrelated to the software you downloaded. Strictly speaking, PUPs are not always malware – PUP developers point out that their programs are downloaded with their users' consent, unlike malware. But it is widely recognized that people mainly download PUPs because they have failed to realize that they have agreed to do so.

PUPs are often bundled with other more legitimate pieces of software. Most people end up with a PUP because they have downloaded a new program and didn't read the small print when installing it – and therefore didn't realize they were opting in for additional programs that serve no real purpose.

PUP malware example:

- **Mindspark malware** – this was an easily installable PUP which ended up on users' machines without them noticing the download. Mindspark can change settings and trigger behavior on the device without the user's knowledge. It is notoriously difficult to eliminate.

Hybrids

Today, most malware is a combination of different types of malicious software, often including parts of Trojans and worms and occasionally a virus. Usually, the malware program appears to the end-user as a Trojan, but once executed, it attacks other victims over the network like a worm.

Hybrid malware example:

- In 2001, a malware developer calling himself 'Lion' released a hybrid malware — a worm/rootkit combination. Rootkits allow hackers to manipulate operating system files, while worms are powerful vectors for rapidly spreading code pieces. This malicious combination caused havoc: it inflicted damage on more than 10,000 Linux systems. Worm/rootkit combination malware was explicitly designed to exploit the vulnerabilities in Linux systems.

Fileless malware

Fileless malware is a type of malicious software that uses legitimate programs to infect a computer. It does not rely on files and leaves no footprint, making it challenging to detect and remove. Fileless malware emerged in 2017 as a mainstream type of attack, but many of these attack methods have been around for a while.

Without being stored in a file or installed directly on a machine, fileless infections go straight into memory, and the malicious content never touches the hard drive. Cybercriminals have increasingly turned to fileless malware as an effective alternative form of attack, making it more difficult for traditional antivirus to detect because of the low footprint and the absence of files to scan.

Fileless malware examples:

- Frodo, Number of the Beast, and The Dark Avenger were all early examples of this type of malware.

Logic bombs

Logic bombs are a type of malware that will only activate when triggered, such as on a specific date and time or on the 20th log-on to an account. Viruses and worms often contain logic bombs to deliver their payload (i.e., malicious code) at a pre-defined time or when another condition is met. The damage caused by logic bombs varies from changing bytes of data to making hard drives unreadable.

Logic bomb example:

- In 2016, a programmer caused spreadsheets to malfunction at a branch of the Siemens corporation every few years, so that they had to keep hiring him back to fix the problem. In this case, nobody suspected anything until a coincidence forced the malicious code out into the open.

How does malware spread?

The most common ways in which malware threats can spread include:

- **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.
- **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.
- **Pop-up alerts:** This includes fake security alerts which trick you into downloading bogus security software, which in some cases can be additional malware.
- **Vulnerabilities:** A security defect in software can allow malware to gain unauthorized access to the computer, hardware, or network.
- **Backdoors:** An intended or unintended opening in software, hardware, networks, or system security.
- **Drive-by downloads:** Unintended download of software with or without knowledge of the end-user.
- **Privilege escalation:** A situation where an attacker obtains escalated access to a computer or network and then uses it to launch an attack.
- **Homogeneity:** If all systems are running the same operating system and connected to the same network, the risk of a successful worm spreading to other computers is increased.
- **Blended threats:** Malware packages that combine characteristics from multiple types of malware, making them harder to detect and stop because they can exploit different vulnerabilities.

Signs of a malware infection

If you've noticed any of the following, you may have malware on your device:

- A slow, crashing, or freezing computer
- The infamous 'blue screen of death'
- Programs opening and closing automatically or altering themselves
- Lack of storage space
- Increased pop-ups, toolbars, and other unwanted programs
- Emails and messages being sent without you initiating them