Malware Types

1. Viruses & Worms

Viruses

Viruses were the most common type of malware in the 1990s with the introduction of Email attachments. One person would open an infected email and the entire company would be infected in short order.

A computer virus is what most of the media and regular end-users call every malware program reported in the news. Fortunately, most malware programs aren't viruses. Pure computer viruses are uncommon today, comprising less than 10 percent of all malware.

A computer virus is the only type of malware that "infects" other files and programs. A virus modifies legitimate data files (like a Word docs) in such a way that when a victim's file is executed (i.e. by opening it in Microsoft Word), the virus is also executed.

This makes viruses particularly hard to clean up because the malware is executed from a legitimate (i.e. non-infected) program. Even the best antivirus programs struggle with removing viruses correctly and in many (if not most) cases will simply quarantine or delete the infected file instead.

Viruses spread through script files, and documents (i.e. attachments) shared through the use of web apps. Viruses are also capable of copying themselves and spreading to other computers. Viruses often spread in this way by attaching themselves to programs and executing code when a user opens a document related to the infected programs.

Viruses can be used to steal information, harm host computers and networks, create botnets, steal money, render advertisements, and more.

Worms

Computer worms can be classified as a type of computer virus, but there are several characteristics that distinguish computer worms from regular viruses. A major difference is that computer worms have the ability to self-replicate and to spread by themselves while viruses rely on human activity to spread (i.e. running a program, opening a file, etc).

Although worms can spread through emails with infected attachments, they usually spread by themselves over computer networks by exploiting operating system vulnerabilities. These vulnerabilities are design weaknesses (logic errors) or bugs (run-time errors) in the code of legitimate programs (e.g. Microsoft Word) or operating systems (e.g. Microsoft Windows).  Worms typically cause harm to their host networks by consuming bandwidth and overloading web servers.

Worms can also contain “payloads” that are intended to cause specific damage host computers. Payloads are pieces of code written to perform actions on affected computers beyond simply spreading the worm. Payloads are commonly designed to steal data, delete files, or create botnets.

Famous viruses & worms in history:

[Iloveyou worm](http://en.wikipedia.org/wiki/ILOVEYOU)

[SQL Slammer](http://www.infoworld.com/t/malware/exorcizing-the-ghost-slammer-492)

[MS Blaster](http://en.wikipedia.org/wiki/Blaster_(computer_worm))

2. Trojans, Rootkits & Botnets

Trojans

Computer worms have been replaced by [Trojan horse](https://www.csoonline.com/article/3403381/what-is-a-trojan-horse-how-this-tricky-malware-works.html) malware programs as the weapon of choice for hackers. Trojans are popular with cyber criminals for two reasons: They're easy to write and they are easy to spread by tricking end-users.

Trojans appear to be legitimate programs, but they contain malicious instructions. The most popular Trojan type is the fake antivirus program, which pops up and claims you're infected, then instructs you to run a program to clean your PC. Users swallow the bait and the Trojan takes root. Trojans also easily spread through web sites that encourage the downloading of pirated software, game patches, and video files. A Trojan must be executed by its victim to do its work.

A Trojan can give an attacker remote access to an infected computer. Once an attacker has access to an infected computer, it is possible for the attacker to steal data (logins, financial data, even electronic money), install more malware, modify files, monitor user activity (screen watching, keylogging, etc), use the computer in botnets, and anonymize internet activity by the attacker.

Rootkits

A [rootkit](https://www.veracode.com/security/rootkit) is a type of stealth program designed to remotely access or control a computer without being detected by users or security programs. A rootkit modifies the underlying operating system to take ultimate control of the computer. Once a rootkit has been installed it is possible for the malicious party behind the rootkit to remotely execute files, access/steal information, modify system configurations, alter software (especially any security software that could detect the rootkit), install concealed malware, or control the computer as part of a botnet.

Rootkit prevention, detection, and removal can be difficult due to their stealthy operation. Because a rootkit continually hides its presence, typical security products are not effective in detecting and removing rootkits. As a result, rootkit detection relies on manual methods such as monitoring computer behavior for irregular activity. Organizations and users can protect themselves from rootkits by regularly patching vulnerabilities in software, applications, and operating systems, updating virus definitions, avoiding suspicious downloads, and performing static analysis scans.

Botnets

Bots are infected computers that become part of a larger malicious network. [Botnets](https://www.csoonline.com/article/3240364/hacking/what-is-a-botnet-and-why-they-arent-going-away-anytime-soon.html) range in size from a few thousand compromised computers to huge networks with hundreds of thousands of systems under the control of a single botnet master. These botnets are often rented out to other criminals who then use them for their own criminal purposes.

Botmasters have one or more "command and control" servers that send out instructions to infected bot computers. Bots can be used for DDoS (Distributed Denial of Service) attacks, as spambots that render advertisements on websites, as web spiders that scrape server data, and for distributing malware disguised as popular search items on download sites. Websites can guard against bots with CAPTCHA tests that verify users as human.

3. Ransomware

Ransomware is a form of malware that essentially holds a computer system captive while demanding a ransom. Ransomware is now the most common type of malware because of its pay off using cryptocurrency and due to its ability to attack large companies, hospitals, police departments, and [even entire cities](https://www.cnn.com/2018/03/27/us/atlanta-ransomware-computers/index.html).

Ransomware typically spreads like a normal computer worm ending up on a computer via a downloaded file or through some other vulnerability in a network service. The malware restricts user access to the computer either by encrypting files on the hard drive or locking down the system and displaying messages that are intended to force the user to pay the malware creator to remove the restrictions and regain access to their computer.

A typical ransomware programs look for and encrypt users’ files within a few minutes of infection. However, some more advanced programs are appearing that take a “wait-and-see” approach. By watching the user for a few hours before setting off the encryption routine, the malware admin can figure out exactly how much ransom the victim can afford and also be sure to delete or encrypt other supposedly safe backups.

Ransomware can be prevented just like every other type of malware program, but once executed, it can be hard to reverse the damage without a good, validated backup. According to some studies, about a quarter of the victims pay the ransom, and of those, about 30 percent still do not get their files unlocked. Either way, unlocking the encrypted files, if even possible, takes particular tools, decryption keys and more than a bit of luck. The best advice is to make sure you have a good, offline backup of all critical files.

4. Adware, Malvertising & Spam

Adware

A[dware](https://www.csoonline.com/article/3406422/what-is-adware-how-it-works-and-how-to-protect-against-it.html) is a form of malware which attempts to expose the end-user to unwanted and potentially malicious advertising. A common adware program might redirect a user's browser searches to look-alike web pages that contain other product promotions.

Adware (short for advertising-supported software) is a type of malware that automatically delivers advertisements. Common examples of adware include pop-up ads on websites and advertisements that are displayed by software. Often times software and applications offer “free” versions that come bundled with adware. Most adware is sponsored or authored by advertisers and serves as a revenue generating tool. While some adware is solely designed to deliver advertisements, it is not uncommon for adware to come bundled with spyware that is capable of tracking user activity and stealing information. Due to the added capabilities of spyware, adware/spyware bundles are significantly more dangerous than adware on its own.

Malvertising

M[alvertising](https://www.csoonline.com/article/3373647/what-is-malvertising-and-how-you-can-protect-against-it.html) is the use of legitimate ads or ad networks to secretly deliver malware to unsuspecting users’ computers. For example, a cybercriminal 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.”

Cybercriminals have also been known to compromise legitimate ad networks that deliver ads to many websites. That’s often how popular websites such as the New York Times, Spotify and the London Stock Exchange have been vectors for malicious ads, putting their users in jeopardy.

The goal of cybercriminals who use malvertising is to make money. Malvertising can deliver any type of money-making malware, including ransomware, cryptomining scripts or banking Trojans.

Spam

Spam is the electronic sending of large numbers of unwanted messages. The most common medium for spam is email, but it is not uncommon for spammers to use instant messages, texting, blogs, web forums, search engines, and social media. While spam is not actually a type of malware, it is very common for malware to spread through spamming. This happens when computers that are infected with viruses, worms, or other malware are used to distribute spam messages containing more malware. Users can prevent getting spammed by avoiding unfamiliar emails and keeping their email addresses as private as possible.

5. Spyware

[Spyware](https://www.csoonline.com/article/3384100/what-is-spyware-how-it-works-and-how-to-prevent-it.html) is most often used by people who want to check on the computer activities of loved ones. Criminals can also use spyware to log the keystrokes of victims and gain access to passwords / account information or financial / intellectual property. Spyware often has additional capabilities as well, ranging from modifying security settings of software or browsers to interfering with network connections.

Spyware spreads by exploiting software vulnerabilities, bundling itself with legitimate software, or in Trojans. Spyware programs are usually the easiest to remove, often because they aren't nearly as hidden in their intentions as other types of malware. A much bigger concern than the actual spyware is the mechanism it used to exploit the computer or user. This is because the presence of a spyware program should serve as a warning that the computer has a weakness that could be exploited by other types of malware.

**6. Fileless malware**

Fileless malware isn’t really a different category of malware, but more of a description of how they exploit and persevere. Traditional malware travels and infects new systems using the file system. Fileless malware, which today comprises over 50 percent of all malware and growing, is malware that doesn’t directly use files or the file system. Instead they exploit and spread in memory only or using other “non-file” OS objects such as registry keys, APIs or scheduled tasks.

Many [fileless attacks](https://www.csoonline.com/article/3227046/malware/what-is-a-fileless-attack-how-hackers-invade-systems-without-installing-software.html" \t "_blank) begin by exploiting an existing legitimate program, becoming a newly launched “sub-process,” or by using existing legitimate tools built into the OS (like Microsoft’s PowerShell). The end result is that fileless attacks are harder to detect and stop. If you aren’t already very familiar with common fileless attack techniques and programs, you probably should be if you want a career in computer security.

In the context of software, a bug is a flaw produces an undesired outcome. These flaws are usually the result of human error and typically exist in the source code or compilers of a program. Minor bugs only slightly affect a program’s behavior and as a result can go for long periods of time before being discovered. More significant bugs can cause crashing or freezing. Security bugs are the most severe type of bugs and can allow attackers to bypass user authentication, override access privileges, or steal data. Bugs can be prevented with developer education, quality control, and code analysis tools.

**Finding and removing malware**

Today, many malware programs start out as a Trojan or worm, but then dial home to a botnet and let human attackers into the victim's computer and network. Many [advanced persistent threat (APT) attacks](http://www.infoworld.com/d/security/5-signs-youve-been-hit-advanced-persistent-threat-204941) start out this way: They use Trojans to gain the initial foothold into hundreds or thousands of companies, while the human attacks lurk, in search of interesting intellectual property. The vast majority of malware exists to steal money — directly out of a bank account or indirectly by stealing passwords or identities.

If you're lucky, you can find malicious executables using a program like [Microsoft's Autoruns](http://technet.microsoft.com/en-us/sysinternals/bb963902.aspx), Microsoft’s Process Explorer, or [Silent Runners](http://www.silentrunners.org/). If the malware program is stealthy, you'll have to remove the hiding component from memory first (if possible), then work on extricating the rest of the program. Often, I'll boot Microsoft Windows into Safe Mode or through another method, remove the suspected stealth component (sometimes by just renaming it), and run a good antivirus scanner a few times to clean up the remainders after the stealth part is removed. Here’s [one good tutorial](http://www.infoworld.com/article/2883958/antimalware/how-to-detect-malware-infection-in-9-easy-steps.html) on how to use Process Explorer to discover and remove malware, and [another here](http://www.infoworld.com/article/3014323/security/a-free-almost-foolproof-way-to-check-for-malware.html).

Unfortunately, finding and removing individual malware program components can be a fool's errand. It's easy to get it wrong and miss a component. Plus, you don't know whether the malware program has modified the system in such a way that it will be impossible to make it completely trustworthy again.

Unless you're well trained in malware removal and forensics, back up the data (if needed), format the drive, and reinstall the programs and data when you find malware on a computer. Patch it well and make sure end-users know what they did wrong. That way, you get a trustworthy computer platform and move ahead in the fight without any lingering risks or questions.

**Malware Symptoms**

While these types of malware differ greatly in how they spread and infect computers, they all can produce similar symptoms. Computers that are infected with malware can exhibit any of the following symptoms:

* Increased CPU usage
* Slow computer or web browser speeds
* Problems connecting to networks
* Freezing or crashing
* Modified or deleted files
* Appearance of strange files, programs, or desktop icons
* Programs running, turning off, or reconfiguring themselves (malware will often reconfigure or turn off antivirus and firewall programs)
* Strange computer behavior
* Emails/messages being sent automatically and without user’s knowledge (a friend receives a strange email from you that you did not send)

**Malware Prevention and Removal**

There are several general best practices that organizations and individual users should follow to prevent malware infections. Some malware cases require special prevention and treatment methods, but following these recommendations will greatly increase a user’s protection from a wide range of malware:

* Install and run anti-malware and firewall software. When selecting software, choose a program that offers tools for detecting, quarantining, and removing multiple types of malware. At the minimum, anti-malware software should protect against viruses, spyware, adware, Trojans, and worms. The combination of anti-malware software and a firewall will ensure that all incoming and existing data gets scanned for malware and that malware can be safely removed once detected.
* Keep software and operating systems up to date with current vulnerability patches. These patches are often released to patch bugs or other security flaws that could be exploited by attackers.
* Be vigilant when downloading files, programs, attachments, etc. Downloads that seem strange or are from an unfamiliar source often contain malware.

eefsdfdsf

#### Virus

A computer virus is a piece of software that can 'infect' a computer, install itself and copy itself to other computers, without the users knowledge or permission. It usually attaches itself to other computer programs, data files, or the boot sector of a Hard drive.

#### Malware

Malware is short for **mal**icious soft**ware**. Malware is the name given to any type of software that could harm a computer system, interfere with and gather a user's data, or make the computer perform actions without the owner's knowledge or permission.

#### Trojan horse

A type of malware that uses malicious code to install software that seems ok, but is hidden to create back doors into a system typically causing loss or theft of data from an external source.

#### Worm

Unlike a virus, a worm, is a standalone piece of malicious software that replicates itself in order to spread to other computers. It often uses a computer network to spread itself, relying on security flaws on the target system to allow access.

#### Spyware

Spyware is software that aids in gathering information about a person or organization without their knowledge, they can monitor and log the activity performed on a target system, like log key strokes, or gather credit card and other information.

#### Adware

Adware is software which can automatically causes pop-up and banner adverts to be displayed in order to generate revenue for its author or publisher. A lot of freeware will use Adware but not always in a malicious way, if it was malicious, it would then be classed as spyware or malware.

9 Types

Here are 9 Computer Viruses that you should know about:

**1. Boot Sector Virus.**

Even though this virus has now become obsolete, it still pops out in one way or the other. This virus got attention when floppy disks were used to boot a computer. In modern computers, this virus could appear on the “Master Boot Record”. In the partitioned storage device of your computer, it is the first sector to take place.

However, thanks to the fact evolution of Internet, the threat of this virus is now mitigated.

From a user perspective, boot sector viruses are some of the most dangerous. Because they infect the master boot record, they are notoriously difficult to remove, often requiring a full system format. This is especially true if the virus has encrypted the boot sector or excessively damaged the code.

They typically spread via removable media. They reached a peak in the 1990s when floppy disks were the norm, but you can still find them on USB drives and in email attachments. Luckily, improvements in BIOS architecture have reduced their prevalence in the last few years.

**2. Web Scripting Virus.**

Similar to the hyperlinks that we used in Microsoft Word, many websites rest on codes to provide engaging content to their users. For example, since the trends of watching videos online have now become very popular – more than 2 Billion Videos are streamed on Facebook every day, these videos also execute a specific code.

These codes can be exploited and it is very troublesome to note that this exploitation has taken place on some very notable sites. All the hackers have to do it to leave a comment in the Comments Section of the website which contains that code. Thus, even without the Webmaster knowing it, the code gets exerted into the site.

**3. Browser Hijacker.**

Ever faced a problem where the homepage of your web page gets automatically directed to a particular site? Well, that is the most common way by which this ransomware hijacks your browser.

While its visual effects might epitomize the threat, this hijacker is nothing more than a tactic to increase income from web ads. However, if you still want to clean your computer from this virus, give [Soft2Secure](http://soft2secure.com/knowledgebase/teslacrypt-3-0) a go.

**4. Resident Virus.**

After inserting itself directing into the memory of your system, this virus has the capability to take a number of actions. One of its more troublesome features is its ability to run away. Leaving behind the file which was originally infected, this virus has the ability to run on its own.

Resident viruses are the other primary type of file infectors. Unlike direct action viruses, they install themselves on a computer. It allows them to work even when the original source of the infection has been eradicated. As such, experts consider them to be more dangerous than their direct action cousin.

Depending on the programming of the virus, they can be [**tricky to spot**](https://www.makeuseof.com/tag/what-is-code-signed-malware/) and even trickier to remove. You can split resident viruses into two areas; fast infectors and slow infectors. Fast infectors cause as much damage as quickly as possible and are thus easier to spot; slow infectors are harder to recognize because their symptoms develop slowly.

In a worst-case scenario, they can even attach themselves to your anti-virus software, infecting every file the software scans. You often need a unique tool—such as an operating system patch—for their total removal. [**An anti-malware app will not be enough to protect you**](https://www.makeuseof.com/tag/antivirus-software-isnt-enough/).

**5. Direct Action Virus.**

Similar to the Vienna virus which shocked computers in 1998, this virus comes into action after you have executed the file. The load is delivered to your computer and the virus becomes active.

However, this virus has a limitation. It takes no action unless the file which is infected gets implemented again.

A direct action virus is one of the two main types of file infector viruses (the other being a resident virus). The virus is considered “non-resident”; it doesn’t install itself or remain hidden in your computer’s memory.

It works by attaching itself to a particular type of file (typically EXE or COM files). When someone executes the file, it springs into life, looking for other similar files in the directory for it to spread to.

On a positive note, the virus does not typically delete files nor hinder your system’s performance. Aside from some files becoming inaccessible, it has a minimal impact on a user and can be easily removed with an anti-virus program.

**6. Polymorphic Virus.**

One of the factors that epitomize the usefulness of this virus is its ability to evade. The Antivirus programs that are enabled on our computers detect the presence of any virus by detecting its code.

Polymorphic virus has exploited this limitation beautifully as it changes its code every time the infected file is executed. Thus, it becomes nearly impossible for any ordinary antivirus to track it down.

According to Symantec, polymorphic viruses are one of the most [**difficult to detect/remove for an anti-virus program**](https://www.makeuseof.com/tag/3-things-antivirus-doesnt-take-care/). It claims anti-virus firms need to “spend days or months creating the detection routines needed to catch a single polymorphic”.

But why are they so hard to protect against? The clue is in the name. Anti-virus software can only blacklist one variant of a virus—but a polymorphic virus changes its signature (binary pattern) every time it replicates. To an anti-virus program, it looks like an entirely different piece of software, and can, therefore, elude the blacklist.

**7. File Infector Virus.**

Although the word “file” in its name might suggest otherwise, this virus does not take the help of files every time. In fact, the file is only the starting point as the file infector dwarfs the first file after which it re-writes the file.

To an end-user, an overwrite virus is one of the most frustrating, even if it’s not particularly dangerous for your system as a whole.

That’s because it will delete the contents of any file which it infects; the only way to remove the virus is to delete the file, and consequently, lose its contents. It can infect both standalone files and entire pieces of software.

Overwrite viruses typically have low visibility and are spread via email, making them hard to identify for an average PC user. They enjoyed a heyday in the early 2000s with Windows 2000 and Windows NT, but you can still find them in the wild.

Also known as “Cavity Viruses”, spacefiller viruses are more intelligent than most of their counterparts. A typical modus operandi for a virus is to simply attach itself to a file, but spacefillers try to get into the empty space which can sometimes be found within the file itself.

This method allows it to infect a program without damaging the code or increasing its size, thus enabling it to bypass the need for the stealthy anti-detection techniques other viruses rely on.

Luckily, this type of virus is relatively rare, though the growth of Windows Portable Executable files is giving them a new lease of life.

**8. Multipartite Virus.**

If you have read carefully the aforementioned viruses, you might have noticed that they use two methods for their transmission. Either they use one method or a single payload is delivered.

However, this virus wants to claim both. Depending upon the operating system of your computer or the files that exist on your computer, it might use any of the two methods to spread.

While some viruses are happy to spread via one method or deliver a single payload, multipartite viruses want it all. A virus of this type may spread in multiple ways, and it may take different actions on an infected computer depending on variables, such as the operating system installed or the existence of certain files.

They can simultaneously infect both the boot sector and executable files, allowing them to act quickly and spread rapidly.

The two-pronged attack makes them tough to remove. Even if you clean a machine’s program files, if the virus remains in the boot sector, it will immediately reproduce once you turn on the computer again.

**9. Macro Virus.**

Appearing in the form of a word document which seemingly links the user to pornographic websites, Melissa is one of the most known Micro Virus. Going one step further, this virus not only exploits the user but also his/her friends by mailing the copies of the infected virus document to the contact list.

If you are handling a website, you can also [keep your website virus and malware-free using Sitelock](https://hostingdecisions.com/what-is-sitelock/). You can also see how to stop cyber attacks with these [Cyber Security Kiosks](https://thelab.olea.com/stop-cyber-attacks-front-door-cyber-security-kiosks/) from Olea.

If you feel that you know another significant type of virus, please feel free to let us know in the comments section.

7 Types

xczxcf

References

<http://www.youngupstarts.com/2016/04/14/9-types-of-computer-viruses-that-you-should-know-about-and-how-to-avoid-them/>

<https://www.veracode.com/blog/2012/10/common-malware-types-cybersecurity-101>

<https://www.csoonline.com/article/2615925/security-your-quick-guide-to-malware-types.html>