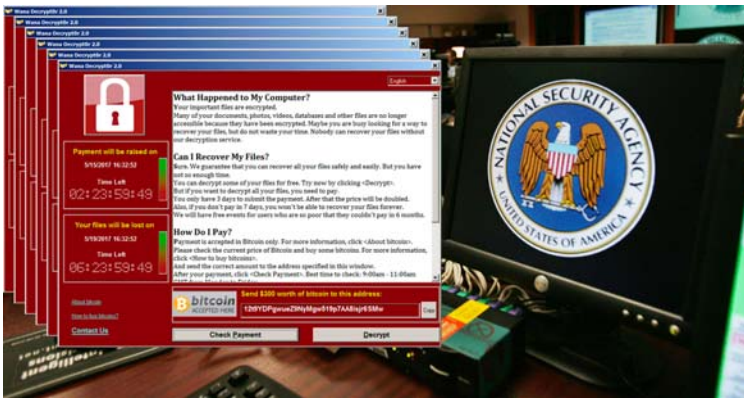
TYPES OF MALWARE

We've all encountered malware at some point. Today, millions of unique programs have been developed to access your system, files, and wallet. While each leaves a different footprint, they all have a common, simple root.
In the modern world, criminal and national hackers threaten everyone's way of life. But in the beginning of malware, there was nothing malicious about it. At that time, the intention was to test computers' real possibilities – not to harm, steal, or manipulate.

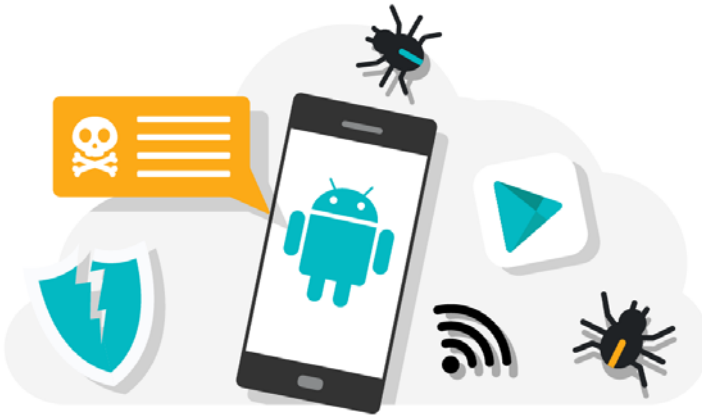


ADWARE

Although rarely malicious, adware can be very irritating as it forces your computer to download or display ads that you don't want to see. This type of malware doesn't typically steal data, but in some cases becomes a real nuisance when, for instance, browser pop-ups can't be closed. Adware can be installed unbeknownst to the user with other applications.

ANDROID MALWARE

Since the majority of smartphones and mobile devices run on Android, and because of the open nature of the Google ecosystem, most malware attacks are focused there. In the usual scenario, the cyber criminals trick users into downloading third-party apps, or even enter the Google Play Store, pretending to offer useful tools or games.



BACKDOOR

Backdoors, a.k.a., secret passages into a system, are very common. Manufacturers may create them either for intentional use by personnel or law enforcement, or unintentionally, with careless coding. Viruses and other malware can create backdoors as well.

BOTS AND BOTNETS

A bot is a software set up to perform automated tasks. Bots can be helpful, as in the case of page indexing for search engines, or when companies use them to answer customer questions. However, when it comes to IT security, a bot is a device infected by malware that makes it execute harmful tasks without the owner's permission. In these terms, a botnet is a network of such devices that hackers often use to send out spam or phishing campaigns or for other malicious tasks. Smart devices using the Internet of Things have recently become target of botnet attacks.

BROWSER HIJACKER

Some types of malware will hijack your browser, changing its behavior. As a result, the browser may acquire a new homepage, several toolbars, a new search engine, or display a multitude of ads. To further the damage, you may even be directed to websites that download more malware to your system.

BUG

Bugs are defects in a piece of software code. They exist in all computer programs, but most are just irksome. However, if bugs are the matter of a security weakness, they can compromise your entire system.

CRIMEWARE

Malware used to commit crimes for financial gain is referred to as 'crimeware'. It encompasses various types of malicious software.

CRYPTOCURRENCY MINER MALWARE

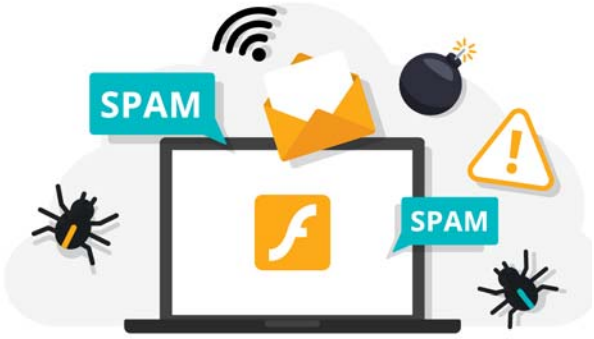
With the rise of cryptocurrency popularity, many people decide to use their computers or web servers to mine for it and make extra cash. However, where money is involved, malware soon follows. Many hackers, in their ambition to mine as much currency as possible, capture others' PC power in botnets for their own purposes. Oftentimes, this kind of theft may render the computer useless to its owner, and the victim is none the wiser of the reason for their loss of processing power. Internet of Things devices have also been targeted for the purposes of illegal financial gain.

FAKE OR ROGUE SECURITY SOFTWARE

The past decade is brimming with cases of fake security software posing as legal antimalware and antivirus programs. By installing this tool, you do more harm than good as you only allow cyber criminals to infect your system, steal your personal information, and then ask you to pay for a clean-up you don't actually need.

FILELESS MALWARE

There is a type of malware that is not file-dependent. In fact, it resides in a computer's memory, not its hard drive – hence its name. Fileless malware is more difficult to detect as it has no files and disappears at reboot.



INTERNET OF THINGS MALWARE

Smart devices, including your router and security cameras, can be quite easily infected by malware – and the damage is usually substantial. With security that is often not sufficient to fight malware attacks, many such IoT devices that we plug at home and forget about can give attackers access to our personal space and information.

KEYLOGGER

Software, which keeps record of all keys that a user presses, is called a keylogger. Cyber criminals often use keyloggers to gain access to account credentials. Some companies also use keyloggers, though their purpose is tracking employee activities for criminal or illegal behavior.

MALVERTISING

Malvertising is not the same as adware, as it operates via real ads and ad networks. However, clicking on such an ad – or, in some cases, even scrolling over it – will download malware to your computer or redirect you to a malicious website. In some cybercriminal attacks, legit ad networks have been used to target the consumers of popular websites, such as major news portals, video and audio databases, or even the London Stock Exchange. Of course, money is at the root of any cybercriminal campaign and malvertising is no different. In fact, with its wide reach, malvertising campaigns can infect thousands of computers, delivering cryptocurrency mining scripts, ransomware, Trojans, and other infections.

MOBILE MALWARE

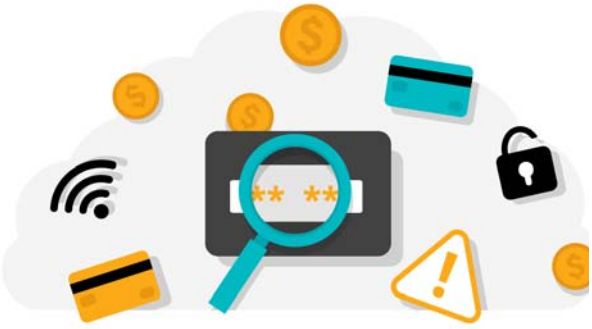
Mobile devices, such as smartphones and tablets, have opened a huge potential for cybercrime. Used daily for data storage, picture taking, conversations, etc., these devices hold information on each and every one of us. No wonder that hackers are working on creating various malware specifically targeting smartphones. If your device is infected, cybercriminals can use it to locate you, spy on your personal life, and blackmail you.

PHISHING AND SOCIAL ENGINEERING

Hackers prefer using email attacks like phishing to trick users into sharing their account credentials, downloading malicious file attachments, or visiting websites that automatically install malware onto their system. Spear phishing works the same way, the only difference being that the targets are narrowed down to a specific user or organization.

RAM SCRAPER

Malware that collects data stored in temporary system memory is known as a RAM scraper. This tool is often used to infect point-of-sale (POS) terminals and steal credit card information before encryption. Many cases have been known, but the most famous ones are the Target and Home Depot breaches in the US.



RANSOMWARE

Ransomware is often used by cybercriminals of our day, attack incidents almost tripling in just under a year. In its essence, this malicious tool locks up your system, allowing no access until a ransom is paid. The threat to non-compliance often involves sharing embarrassing or personal data in social media and other portals. Since no one wants their ugly side out in the open, cybercriminals have collected billions of dollars this way.

Real life example

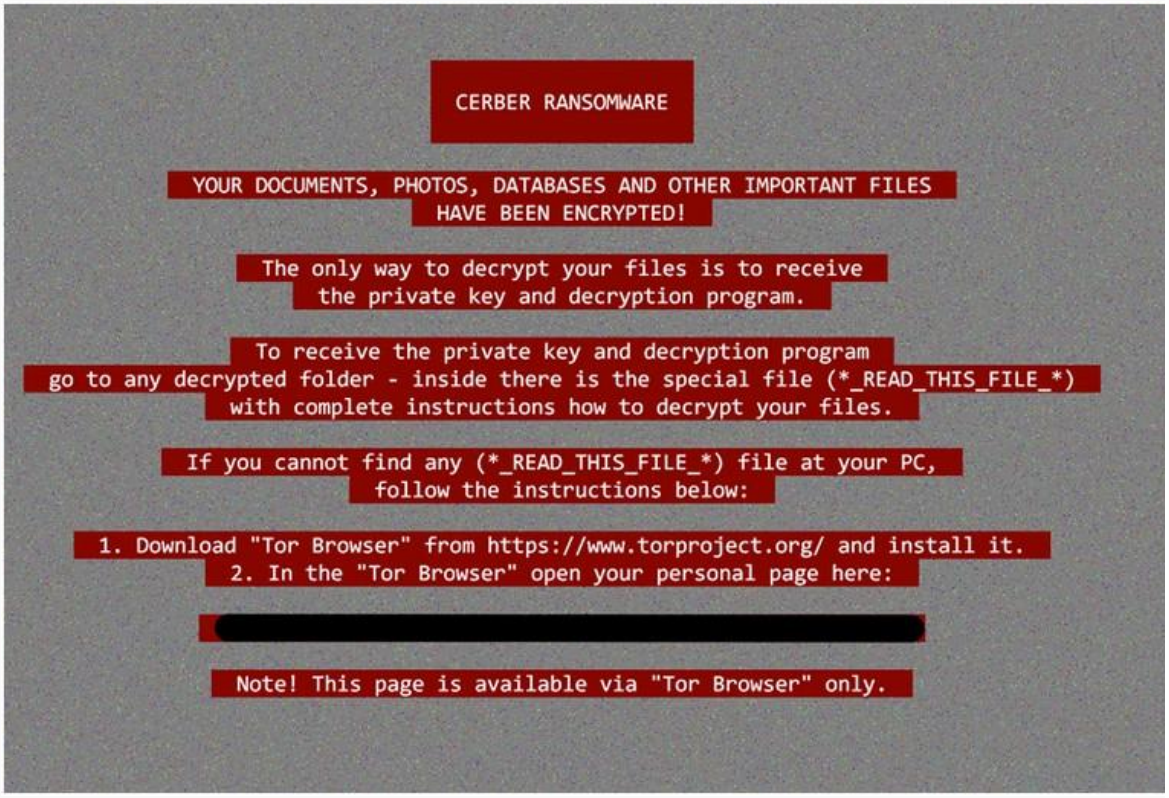


Image: Malwarebytes “Ransomware demands a payment in return for returning encrypted files.”

ROOTKIT

Rootkits are hacker tools that hijack admin access to your system. Naturally, this allows them to do anything they want without your knowledge or permission, including meddling with your settings, recording your activity, targeting other systems, etc. Examples include Stuxnet and Flame.

SPAM

Spam refers to that junk mail that you never want to see in your inbox. It usually consists of unsolicited ads, but it can also be harmful as attackers can use it for fraud, or to send infected links or attachments.

SPYWARE

Software used to collect information on a person or an organization without their permission is known as spyware. It can range from malicious when stealing of information is involved, to common website tracking cookies, to official spying on crime suspects or foreign governments.

TROJAN

Taking its name from the mythological Trojan horse in Hellenistic times, this kind of malware enters your system under false pretense. Once on board, it can destroy your hard drive, steal your data, open backdoors for other harmful malware, etc.

Trojans are distributed via email or when visiting infected websites. They need to be downloaded and executed in order to become harmful, and the way they accomplish that is by tricking you. The most common type of Trojan is the fake antivirus program which claims your machine is infected and demands you run a program to get rid of the virus.

Common examples of Trojans include:

- Remote Access Trojans: Tools that give hackers remote access to your system.
- Data Sending Trojans: They collect data from your machine and send it over to the attacker.
- Destructive Trojans: Eliminate your files and services.
- Security Software Disabler Trojans: Render your machine completely vulnerable to malicious software by disabling all system security chann

VIRUS

A virus is a type of malware that requires user interaction to run and spread onto other programs and systems. It may or may not covertly use your system in a botnet, to send out spam, steal account credentials or credit card information, or lock your system entirely. Once they enter a system, computer viruses infect other files and programs making them difficult to clean up. Antivirus programs can rarely reverse the damage, which is why their usual approach is to quarantine or simply delete the infected file.

The most common types of viruses are:

- File viruses: They infect executables which then spread the damage onto other files upon running.
- Macro viruses: Usually contained in Excel macros, these viruses get activated upon a macro execution, then spread to infect other files.

- Master boot record viruses: In the hands of these viruses, you lose your boot records and your system becomes useless.
- Polymorphic viruses: To evade detection, many viruses are coded to change form.
- Stealth viruses: Hard to track down as they lay low among legitimate files or services.
- Multipartite viruses: Hybrids that infect program files and upon execution meddle with the boot record. Upon system reload, the virus contaminates the memory and spreads all over your system.

WIPER-MALWARE

Malware which exists for the sole purpose of irreversibly destroying or erasing all data from a targeted machine or network is known as wiper malware. Sometimes data is wiped after secretly retrieving it from the targeted PC. In other cases, no information is saved prior to the attack. Petya ransomware is one such example from recent years. Initially believed to be a type of ransomware, users and researchers soon realized that no amount of payment would save their data from destruction by Petya.

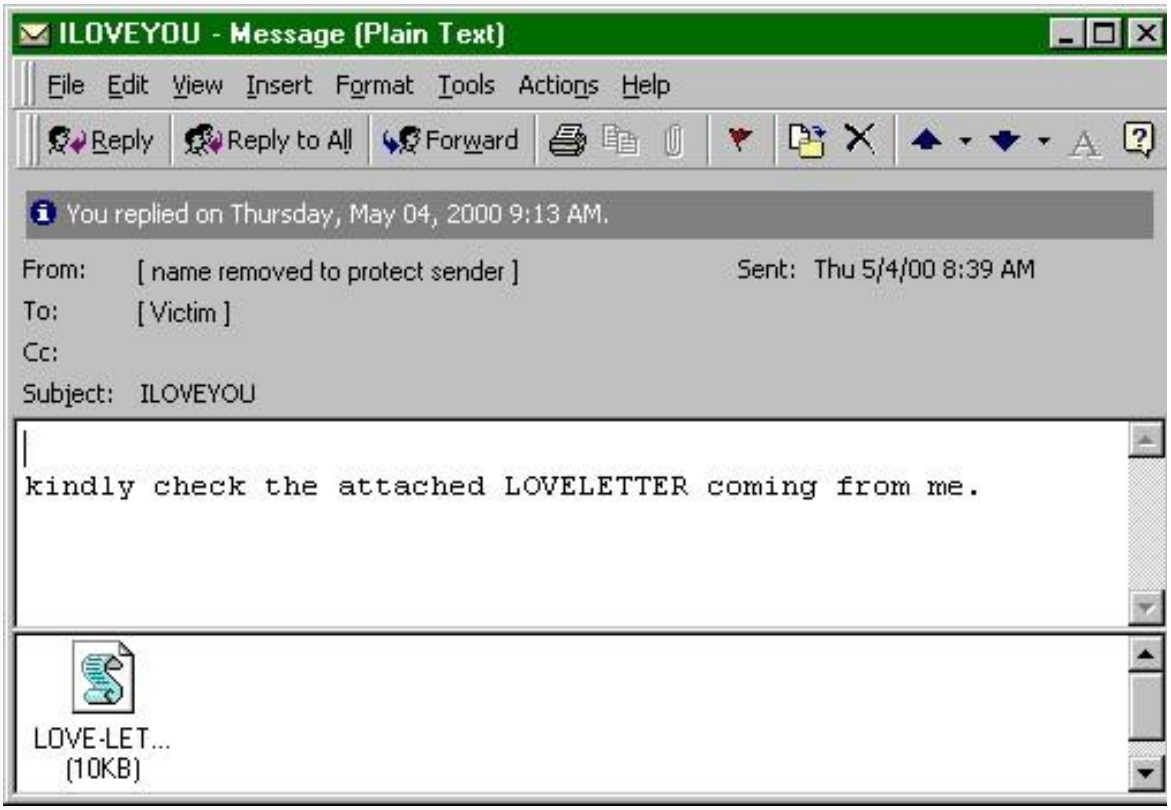
WORM

A worm needs no outside intervention to spread as it exploits other programs to kick start it. Although it doesn't infect other files or programs like a virus, this standalone malware is notorious when it comes to spreading from one system or network to another, causing havoc where it passes.

Starting its development back in ancient mainframe days, worms became most popular with the rise of email communication at the end of the 20th century. Their most usual form of delivery was wormed email attachments, which, once opened, would easily spread over an entire organization via simple self-replication.

One such example was the ILoveYou worm, which affected the entire globe, overloading TV & phone networks, and even people's daily routine.

Real life example



Another worm, SQL Slammer, exploited a Microsoft SQL vulnerability which had been covered by a patch. However, this worm was capable of infecting every unpatched SQL server on the Internet in just 10 minutes.