Types of Malware

Malware, or malicious software, is any program or file that harms a computer or its user. Common types of malware include computer viruses, ransomware, worms, trojan horses and spyware. These malicious programs can steal, encrypt or delete sensitive data, alter or hijack key computing functions and to monitor the victim's computer activity.

Cybercriminals use a variety of physical and virtual means to infect devices and networks with malware. For example, WannaCry, a famous ransomware attack was able to spread by exploiting a known vulnerability. Phishing is another common malware delivery method where emails disguised as legitimate messages contain malicious links or email attachments that deliver executable malware to unsuspecting users.

Sophisticated malware attacks use a command-and-control server to allow attackers to communicate with the infected computer system, steal sensitive information from the hard drive or gain remote access to the device.

1. What are computer viruses?

A virus is a type of malware that, when executed, self-replicates by modifying other computer programs and inserting their own code. When this replication succeeds, the affected areas are then said to be infected.

Virus writers use social engineering and exploit vulnerabilities to infect systems and spread the virus. The Microsoft Windows and Mac operating systems are the targets of the vast majority of viruses that often use complex anti-detection strategies to evade antivirus software.

Viruses are created to make profit (e.g. ransomware), send a message, personal amusement, demonstrate vulnerabilities exist, sabotage and denial of service, or to simply explore cybersecurity issues, artificial life and evolutionary algorithms.

Computer viruses cause billions of dollars worth of economic damage by causing system failure, wasting resources, corrupting data, increasing maintenance costs, logging keystrokes and stealing personal information (e.g. credit card numbers).

2. What is a computer worm?

A computer worm is a self-replicating malware program whose primary purpose is to infect other computers by duplicating itself while remaining active on infected systems.

Often, worms use computer networks to spread, relying on vulnerabilities or security failures on the target computer to access it. Worms almost always cause at least

some harm to a network, even if only by consuming bandwidth. This is different to viruses which almost always corrupt or modify files on the victim's computer.

WannaCry is a famous example of a ransomware cryptoworm that spread without user action by exploiting the EternalBlue vulnerability.

While many worms are designed to only spread and not change systems they pass through, even payload-free worms can cause major disruptions. The Morris worm and Mydoom caused major disruptions by increasing network traffic despite their benign nature.

3. What is a trojan horse?

A trojan horse or trojan is any malware that misleads users of its true intent by pretending to be a legitimate program. The term is derived from the Ancient Greek story of the deceptive Trojan Horse that led to the fall of the city of Troy.

Trojans are generally spread with social engineering such as phishing.

For example, a user may be tricked into executing an email attachment disguised to appear genuine (e.g. an Excel spreadsheet). Once the executable file is opened, the trojan is installed.

While the payload of a trojan can be anything, most act as a backdoor giving the attacker unauthorized access to the infected computer. Trojans can give access to personal information such as internet activity, banking login credentials, passwords or personally identifiable information (PII). Ransomware attacks are also carried out using trojans.

Unlike computer viruses and worms, trojans do not generally attempt to inject malicious code into other files or propagate themselves.

4. What are rootkits?

A rootkit is a collection of malware designed to give unauthorized access to a computer or area of its software and often masks its existence or the existence of other software.

Rootkit installation can be automated or the attacker can install it with administrator access.

Access can be obtained by a result of a direct attack on the system, such as exploiting vulnerabilities, cracking passwords or phishing.

Rootkit detection is difficult because it can subvert the antivirus program intended to find it. Detection methods include using trusted operating systems, behavioural methods, signature scanning, difference scanning and memory dump analysis.

Rootkit removal can be complicated or practically impossible, especially when rootkits reside in the kernel. Firmware rootkits may require hardware replacement or specialized equipment.

5. What is Ransomware?

Ransomware is a form of malware, designed to deny access to a computer system or data until ransom is paid. Ransomware spreads through phishing emails, malvertising, visiting infected websites or by exploiting vulnerabilities.

Ransomware attacks cause downtime, data leaks, intellectual property theft and data breaches.

Ransom payment amounts range from a few hundred to hundreds of thousands of dollars. Payable in cryptocurrencies like Bitcoin.

6. What is keylogger?

Keyloggers, keystroke loggers or system monitoring are a type of malware used to monitor and record each keystroke typed on a specific computer's keyboard. Keyloggers are also available for smartphones.

Keyloggers store gathered information and send it to the attacker who can then extract sensitive information like login credentials and credit card details.

7. What is spyware?

Spyware is malware that gathers information about a person or organization, sometimes without their knowledge, and sends the information to the attacker without the victim's consent.

Spyware usually aims to track and sell your internet usage data, capture your credit card or bank account information or steal personally identifiable information (PII).

Some types of spyware can install additional software and change the settings on your device. Spyware is usually simple to remove because it is not as nefarious as other types of malware.

8. What is adware?

Adware is a type of grayware designed to put advertisements on your screen, often in a web browser or popup.

Typically it distinguishes itself as legitimate or piggybacks on another program to trick you into installing it on your computer, tablet or smartphone.

Adware is one of the most profitable, least harmful forms of malware and is becoming increasingly popular on mobile devices. Adware generates revenue by automatically displaying advertisement to the user of the software.

9. What are bots and botnets?

A bot is a computer that is infected with malware that allows it to be remotely controlled by an attacker.

The bot (or zombie computer) can then be used to launch more cyber attacks or become part of a botnet (a collection of bots).

Botnets are a popular method for distributed denial of service (DDoS) attacks, spreading ransomware, keylogging and spreading other types of malware.

10. What is a backdoor?

A backdoor is a covert method of bypassing normal authentication or encryption in a computer, product, embedded device (e.g. router) or other part of a computer.

Backdoors are commonly used to secure remote access to a computer or gain access to encrypted files.

From there, it can be used to gain access to, corrupt, delete or transfer sensitive data.

Backdoors can take the form a hidden part of a program (a trojan horse), a separate program or code in firmware and operating systems.

Further, backdoors can be created or widely known. Many backdoors have legitimate use cases such as the manufacturer needing a way to reset user passwords.

11. What is a browser hijacker?

A browser hijacker or hijackware changes the behavior of a web browser by sending the user to a new page, changing their home page, installing unwanted toolbars, displaying unwanted ads or directing users to a different website.

12. What is crimeware?

Crimeware is a class of malware designed to automate cybercrime.

It is designed to perpetrate identity theft through social engineering or stealth to access the victim's financial and retail accounts to steal funds or make unauthorized transactions. Alternatively, it may steal confidential or sensitive information as part of corporate espionage.

How does malware spread?

There are six common ways that malware spreads:

1. **Vulnerabilities:** A security defect in software allows malware to exploit it to gain unauthorized access to the computer, hardware or network
2. **Backdoors:** An intended or unintended opening in software, hardware, networks or system security
3. **Drive-by downloads:** Unintended download of software with or without knowledge of the end user
4. **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
5. **Privilege escalation:** A situation where an attacker gets escalated access to a computer or network and then uses it to mount an attack
6. **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 Malware On Your Computer

1. Your PC becomes slow and unresponsive
2. Your PC crashes and restarts frequently
3. Applications on your PC crash frequently
4. Your PC's storage is inaccessible or corrupted
5. You see unusual error messages on your PC
6. You see unwanted popup messages
7. Your Browser Keeps Getting Redirected
8. An Unknown App Sends Scary Warnings
9. Mysterious Posts Appear on Your Social Media
10. You Get Ransom Demands
11. Your System Tools Are Disabled

How to find and remove malware

Prevention is key. Keep your systems patched, continuously monitor for vulnerabilities and educate your staff on the dangers of executing attachments and programs from suspicious emails. And remember, third-party risk and fourth-party risk exist.

You need to make sure your third-party risk management framework and vendor risk management program forces your vendors to keep their systems secure and free of malware like you do. Customers don't care whether it was you or your vendors who caused a data breach or data leak.

How to Protect Your PC Against Malware

Malware can run in the background, and you cannot find it unless you have the best antivirus or virus removal software. This is also applicable to an organization with multiple endpoints operating at various locations.

The best way to protect your PC from malware is to install antivirus software and keep your PC's operating system up-to-date by downloading regular security patches and updates.

When it comes to an organization's security, antivirus products are not a viable option. The ideal way to disarm even the most potent malware is to have an advanced endpoint protection system.

Ten Best Practices for Combating Malware

1. Implementing first-line-of-defense tools that can scale, such as cloud security platforms
2. Adhering to policies and practices for application, system, and appliance patching
3. Employing network segmentation to help reduce outbreak exposures
4. Adopting next-generation endpoint process monitoring tools
5. Accessing timely, accurate threat intelligence data and processes that allow that data to be incorporated into security monitoring and eventing
6. Performing deeper and more advanced analytics
7. Reviewing and practicing security response procedures
8. Backing up data often and testing restoration procedures—processes that are critical in a world of fast-moving, network-based ransomware worms and destructive cyber weapons
9. Conducting security scanning of microservice, cloud service, and application administration systems
10. Reviewing security systems and exploring the use of SSL analytics and, if possible, SSL decryption

Types of Viruses

A virus is a fragment of code embedded in a legitimate program. Virus are self-replicating and are designed to infect other programs. They can wreak havoc in a system by modifying or destroying files causing system crashes and program malfunctions. On reaching the target machine a virus dropper(usually trojan horse) inserts the virus into the system.

Various types of virus :

1. **File Virus :** This type of virus infects the system by appending itself to the end of a file. It changes the start of a program so that the control jumps to its code. After the execution of its code, the control returns back to the main program. Its execution is not even noticed. It is also called **Parasitic virus** because it leaves no file intact but also leaves the host functional.

2. **Boot sector Virus :** It infects the boot sector of the system, executing every time system is booted and before operating system is loaded. It infects other bootable media like floppy disks. These are also known as **memory virus** as they do not infect file system.

3. **Macro Virus:** Unlike most virus which are written in low-level language (like C or assembly language), these are written in high-level language like Visual Basic. These viruses are triggered when a program capable of executing a macro is run. For example, macro virus can be contained in spreadsheet files.
4. **Email viruses**, which constitute the majority of computer viruses, consists of malicious code that is distributed in email messages, and it can be activated when a user clicks on a link in an email message, downloads an email attachment or interacts in some other way with the body of an infected email.

   Virus email are usually programmed to be sent to everyone in the victim's address book once his or her computer has been infected, and tend to proliferate very quickly as a result.

   Viruses are commonly linked to phishing attacks, in which threat actors send out fraudulent emails that appear as if they have been sent from authorized sources with the goal of deceiving users into sharing sensitive information. Spam and malware emails are also very effective at infecting systems and compromising networks.

5. **Multipartite viruses:** This type of virus can spread in various ways and can behave in a different manner depending on factors such as a PC's operating system. These viruses can infect the boot sector as well as files on a computer and can spread extremely rapidly and be very difficult to remove as a result.
6. **Polymorphic viruses:** This type of virus changes its signature when it reproduces, masquerading as a different and seemingly harmless file. These viruses are especially threatening because antivirus programs have a very hard time detecting them. Because traditional antivirus software can only blacklist a single virus variant, many programs take months to identify a single polymorphic virus.

How Antivirus Software Works: 4 Detection Techniques

An antivirus tool is an essential component of most anti-malware suites. It must identify known and previously unseen malicious files with the goal of blocking them before they can cause damage. Though tools differ in the implementation of malware-detection mechanisms, they tend to incorporate the same virus detection techniques. Familiarity with these techniques can help you understand how antivirus software works.

Malware detection techniques employed by antivirus tools can be classified as follows:

Signature-based detection uses key aspects of an examined file to create a static fingerprint of known malware. The signature could represent a series of bytes in the file. It could also be a cryptographic hash of the file or its sections. This method of detecting malware has been an essential aspect of antivirus tools since their inception; it remains a part of many tools to date, though its importance is diminishing. A major limitation of signature-based detection is that, by itself, this method is unable to flag malicious files for which signatures have not yet been developed. With this in mind, modern attackers frequently mutate their creations to retain malicious functionality by changing the file's signature.

Heuristics-based detection aims at generically detecting new malware by statically examining files for suspicious characteristics without an exact signature match. For instance, an antivirus tool might look for the presence of rare instructions or junk code in the examined file. The tool might also emulate running the file to see what it would do if executed, attempting to do this without noticeably slowing down the system. A single suspicious attribute might not be enough to flag the file as malicious. However, several such characteristics might exceed the expected risk threshold, leading the tool to classify the file as malware. The biggest downside of heuristics is it can inadvertently flag legitimate files as malicious.

Behavioral detection observes how the program executes, rather than merely emulating its execution. This approach attempts to identify malware by looking for suspicious behaviors, such as unpacking of malcode, modifying the hosts file or observing keystrokes. Noticing such actions allows an antivirus tool to detect the presence of previously unseen malware on the protected system. As with heuristics, each of these actions by itself might not be sufficient to classify the program as malware. However, taken together, they could be indicative of a malicious program. The use of behavioral techniques brings antivirus tools closer to the category of host intrusion prevention systems (HIPS), which have traditionally existed as a separate product category.

Cloud-based detection identifies malware by collecting data from protected computers while analyzing it on the provider's infrastructure, instead of performing the analysis locally. This is usually done by capturing the relevant details about the file and the context of its execution on the endpoint, and providing them to the cloud engine for processing. The local antivirus agent only needs to perform minimal processing. Moreover, the vendor's cloud engine can derive patterns related to malware characteristics and behavior by correlating data from multiple systems. In contrast, other antivirus components base decisions mostly on locally observed attributes and behaviors. A cloud-based antivirus engine allows

individual users of the tool to benefit from the experiences of other members of the community.

About Virus Total Website:

VirusTotal is a website created by the Spanish security company HispasecSistemas. Launched in June 2004, it was acquired by Google Inc. in September 2012. The company's ownership switched in January 2018 to Chronicle, a subsidiary of Alphabet Inc.

VirusTotal inspects items with over 70 antivirus scanners and URL/domain blacklisting services.

VirusTotal aggregates many antivirus products and online scan engines to check for viruses that the user's own antivirus may have missed, or to verify against any false positives. Files up to 550 MB can be uploaded to the website, or sent via email (max. 32MB). Anti-virus software vendors can receive copies of files that were flagged by other scans but passed by their own engine, to help improve their software and, by extension, VirusTotal's own capability. Users can also scan suspect URLs and search through the VirusTotal dataset. VirusTotal for dynamic analysis of malware uses the Cuckoo sandbox.

Any user can select a file from their computer using their browser and send it to VirusTotal. VirusTotal offers a number of file submission methods, including the primary public web interface, desktop uploaders, browser extensions and a programmatic API. The web interface has the highest scanning priority among the publicly available submission methods. Submissions may be scripted in any programming language using the HTTP-based public API.

As with files, URLs can be submitted via several different means including the VirusTotal webpage, browser extensions and the API.

Upon submitting a file or URL basic results are shared with the submitter, and also between the examining partners, who use results to improve their own systems. As a result, by submitting files, URLs, domains, etc. to VirusTotal you are contributing to raise the global IT security level.

This core analysis is also the basis for several other features, including the VirusTotal Community: a network that allows users to comment on files and URLs and share notes with each other. VirusTotal can be useful in detecting malicious content and also in identifying false positives -- normal and harmless items detected as malicious by one or more scanners.

VirusTotal is free to end users for non-commercial use.

The 7 Best Antivirus Software of 2020

- **Best** Overall: Bitdefender **Antivirus** Plus.
- **Best** for Windows: Norton 360 With LifeLock.
- **Best** for Mac: Webroot SecureAnywhere for Mac.
- **Best** for Multiple Devices: McAfee **Antivirus** Plus.
- **Best** for Free: Kaspersky Free **Antivirus**.
- **Best** Premium Option: Trend Micro Antivirus+ Security.
- **Best** Malware Scanning: Malwarebytes.