MODULE 3: MALICIOUS SOFTWARE

-By
Asst Prof. Rohini Sawant

Malicious programs

- Software threats to computer systems:
- Malicious programs that exploit vulnerabilities in computer systems to launch attacks on security and privacy;
- Continuous development new types of malicious programs and countermeasures;
- Important features: propagation and self-replication;
- Vulnerabilities in computer systems are almost inevitable due to their immense complexity.

Malicious Software

- Malware is short form for malicious software.
- It is a software used or created to disrupt computer operation, gather sensitive information, or gain access to private computer systems.
- It can appear in the form of code, scripts, active content, and other software.
- Malware' is a general term used to refer to a variety of forms of hostile, intrusive, or annoying software.
- Today, malware is used primarily to steal sensitive personal, financial, or business information for the benefit of others. Malware is sometimes used broadly against government or corporate websites to gather guarded information, or to disrupt their operation in general. However, malware is often used against individuals to gain personal information such as social security numbers, bank or credit card numbers, and so on.

Terminology related to Malware

- Installation: How the malware reaches the system eg: attachments
- Detection and Removal: How the malware's presence can be detected rf: Antivirus, Antimalware.
- Payload: Actual function that the malware performs eg: Deletion of files.
- Trigger: Event that invokes the malware eg: clicking a file.
- Replication: Capability of the malware to further replicate or copy itself and infect other systems.
- Eradication: The malware might remove itself after delivering payload.

Types of Malwares

- Viruses
- Trojan horses
- Worms
- Spyware
- Zombie
- Phishing
- Spam
- Adware
- Ransomware

VIRUSES

- A computer virus is a type of malicious software, or malware, that spreads between computers and causes damage to data and software.
- Computer viruses aim to disrupt systems, cause major operational issues, and result in data loss and leakage.
- A key thing to know about computer viruses is that they are designed to spread across programs and systems.
- Computer viruses typically attach to an executable host file, which results in their viral codes executing when a file is opened.

SYMPTOMS OF INFECTION

Given below are such signs which may help you identify computer viruses:

- **Speed of the System –** In case a virus is completely executed into your device, the time taken to open applications may become longer and the entire system processing may start working slowly
- **Pop-up Windows –** One may start getting too many pop up windows on their screen which may be virus affected and harm the device even more
- **Self Execution of Programs –** Files or applications may start opening in the background of the system by themselves and you may not even know about them
- **Log out from Accounts –** In case of a virus attack, the probability of accounts getting hacked increase and password protected sites may also get hacked and you might get logged out from all of them
- **Crashing of the Device –** In most cases, if the virus spreads in maximum files and programs, there are chances that the entire device may crash and stop working

TYPES OF VIRUSES

Resident Virus: Viruses propagate themselves by infecting applications on a host computer. A resident virus achieves this by infecting applications as they are opened by a user. A non-resident virus is capable of infecting executable files when programs are not running.

Multipartite Virus: A multipartite virus uses multiple methods to infect and spread across computers. It will typically remain in the computer's memory to infect the hard disk, then spread through and infect more drives by altering the content of applications. This results in performance lag and application memory running low. Multipartite viruses can be avoided by not opening attachments from untrusted sources and by installing trusted antivirus software.

Direct Action: A direct action virus accesses a computer's main memory and infects all programs, files, and folders located in the autoexec.bat path, before deleting itself. This virus typically alters the performance of a system but is capable of destroying all data on the computer's hard disk and any USB device attached to it. Direct action viruses can be avoided through the use of antivirus scanners. They are easy to detect, as is restoring infected files.

TYPES OF VIRUSES

Browser Hijacker: A browser hijacker manually changes the settings of web browsers, such as replacing the homepage, editing the new tab page, and changing the default search engine. Technically, it is not a virus because it cannot infect files but can be hugely damaging to computer users, who often will not be able to restore their homepage or search engine. It can also contain adware that causes unwanted pop-ups and advertisements. Browser hijackers typically attach to free software and malicious applications from unverified websites or app stores, so only use trusted software and reliable antivirus software.

File Infector: A file infector is one of the most common computer viruses. It overwrites files when they are opened and can quickly spread across systems and networks. It largely affects files with .exe or .com extensions. The best way to avoid file infector viruses is to only download official software and deploy an antivirus solution.

Network Virus: Network viruses are extremely dangerous because they can completely cripple entire computer networks. They are often difficult to discover, as the virus could be hidden within any computer on an infected network. These viruses can easily replicate and spread by using the internet to transfer to devices connected to the network. Trusted, robust antivirus solutions and advanced firewalls are crucial to protecting against network viruses.

TYPES OF VIRUSES

- **Boot Sector Virus:** A boot sector virus targets a computer's master boot record (MBR). The virus injects its code into a hard disk's partition table, then moves into the main memory when a computer restarts. The presence of the virus is signified by boot-up problems, poor system performance, and the hard disk becoming unable to locate. Most modern computers come with boot sector safeguards that restrict the potential of this type of virus.
- **Macro virus:**It is a computer virus written in the same macro language used to create software programs such as Microsoft Excel or Word. It centers on software applications and does not depend on the operating system (OS). As a result, it can infect any computer running any kind of OS, including Windows, macOS and Linux.

WORM

- A worm refers to a malicious program that replicates itself, automatically spreading through a network. In this definition of computer worms, the worm exploits vulnerabilities in your security software to steal sensitive information, install backdoors that can be used to access the system, corrupt files, and do other kinds of harm.
- Worms consume large volumes of memory, as well as bandwidth. This results in servers, individual systems, and networks getting overloaded and malfunctioning. A worm is different from a virus, however, because a worm can operate on its own while a virus needs a host computer.
- It works on law of exponential growth.
- To get a worm in a computer, the worm is often transmitted through vulnerabilities in software. They could also be sent through email attachments or within instant messages or spam emails. After a file is opened, it may link the user to a malicious website or it could download the worm to the user's device automatically. After the worm is on the device, it infects it without the user being able to tell.
- Worms have the ability to delete and modify files. They can also inject more malicious software into a workstation or other device. Sometimes, the worm's primary mission is to replicate itself again and again—simply to waste system resources, like bandwidth or hard drive space. Worms can also steal sensitive data and pave a way for a hacker to get into the computer by installing a backdoor they can access.

Steps for Worm Mitigation

Step 1: Containment: The first step in mitigating a worm attack is to move swiftly to contain the spread of the worm and determine which machines are infected, and whether these devices are patched or unpatched. Infected machines must be isolated from machines that are not yet infected.

Step 2: Inoculation: Once it is clear which parts of the network the worm has infected, and those parts have been contained, other vulnerable systems must be scanned and patched. Patching the vulnerabilities the worm is using to spread will help contain the attack.

Step 3: Quarantine: In this third step of worm mitigation, infected machines are isolated and then disconnected and removed from the network. If removal is not possible, then the infected machines need to be blocked from connecting to and accessing the network.

Step 4: Treat: This last step in the worm mitigation process involves remediating from the attack as well as addressing any other necessary patching of machines and systems. Depending on the severity of the attack, infected systems may need to be reinstalled entirely to ensure a thorough cleanup from the event.

Types of Worm

Email-Worm: An email-worm refers to a worm that is able to copy itself and spread through files attached to email messages.

IM-Worm: An Instant Messenger (IM) worm is a kind of worm that can spread through IM networks. When an IM-worm is operating, it typically finds the address book belonging to the user and tries to transmit a copy of itself to all of the person's contacts.

Net-Worm: A net-worm refers to a kind of worm that can find new hosts by using shares made over a network. This is done using a server or hard drive that multiple computers access via a local-area network (LAN).

P2P-Worm: A P2P-worm is spread through peer-to-peer (P2P) networks. It uses the P2P connections to send copies of itself to users.

SPAM

- Spam email is unsolicited and unwanted junk email sent out in bulk to an indiscriminate recipient list. Typically, spam is sent for commercial purposes. It can be sent in massive volume by botnets, networks of infected computers.
- The classic definition of spam is unsolicited bulk messages, that is, messages sent to multiple recipients who did not ask for them.
- Often, spam email is sent for commercial purposes. While some people view it as unethical, many businesses still use spam. The cost per email is incredibly low, and businesses can send out mass quantities consistently. Spam email can also be a malicious attempt to gain access to your computer.
- The original impetus for spam was advertising. Some spam also does non-commercial advertising. There has always been a modest amount of religious spam, and surges of political spam before elections.
- The other major use of spam is phishing, impersonating a trusted party to steal the victim’s credentials. Phish spam often pretends to be from banks, ISPs, or mail providers, telling victims to confirm or update their accounts

TYPES OF SPAMS

- **Commercial advertisements:** Whether an email message is spam or a legitimate advertisement, in the United States it's subject to the guidelines in the CAN-SPAM act. When businesses capture your email address, they often subscribe you to their newsletter by default, as a low-cost way to sell their products. Whenever you fill out an online form, look for a checkbox to opt into or out of marketing email. While these emails can be pesky, most are harmless, and by law they must have a visible opt-out or unsubscribe option. If you unsubscribe and continue to receive spam, update your email settings to filter messages from the sender's address out of your inbox.
- **Antivirus warnings:** Ironically, antivirus warnings are a common spam tactic. These emails warn you about a computer virus infection and offer a solution--often an antivirus scan--to fix the alleged cyber threat. But taking the bait and clicking the link can grant the hacker access to your system or may download a malicious file. If you suspect that your computer is infected, do not click a random email link. Instead, pursue legitimate cybersecurity software solutions to protect your endpoints.
- **Sweepstakes winners:** Spammers often send emails claiming that you have won a sweepstakes or a prize. They urge you to respond quickly to collect your prize, and may ask you to click a link or submit some personal information. If you don't recognize the competition, or if the email address seems dubious, don't click any links or reply with any personal details.

TYPES OF SPAMS

- **Money scams:** Unfortunately, spammers prey on people's goodwill. A common money scam begins with emails asking for help in dire circumstances. The spammer fabricates a story about needing funds for a family emergency or a tragic life event. Some scams, like the Nigerian prince scheme, promise to give you money if you just send your bank account information or pay a small processing fee. Always be cautious about providing personal information or sending money.
- **Email spoofing:** Why are phishing email scams often effective? Because the spam emails masterfully mimic legitimate corporate messages to get you to act. In a spoofing attack a spammer picks a company brand victims will trust, such as a bank or an employer, then uses the company's exact formatting and logos. Before you reply or click anything, check the From line to make sure that the sender's email address (not just the alias) is legitimate. When in doubt, contact the company to verify whether the email is real.

TROJAN HORSE

- A Trojan Horse Virus is a type of malware that downloads onto a computer disguised as a legitimate program.
- The delivery method typically sees an attacker use social engineering to hide malicious code within legitimate software to try and gain users' system access with their software.
- A simple way to answer the question "what is Trojan" is it is a type of malware that typically gets hidden as an attachment in an email or a free-to-download file, then transfers onto the user’s device.
- Once downloaded, the malicious code will execute the task the attacker designed it for, such as gain backdoor access to corporate systems, spy on users’ online activity, or steal sensitive data.
- Indications of a Trojan being active on a device include unusual activity such as computer settings being changed unexpectedly.

HOW TROJAN SPREADS

- Unlike computer viruses, a Trojan horse cannot manifest by itself, so it needs a user to download the server side of the application for it to work. This means the executable (.exe) file should be implemented and the program installed for the Trojan to attack a device's system. A Trojan virus spreads through legitimate-looking emails and files attached to emails, which are spammed to reach the inboxes of as many people as possible. When the email is opened and the malicious attachment is downloaded, the Trojan server will install and automatically run every time the infected device is turned on.
- Devices can also be infected by a Trojan through social engineering tactics, which cyber criminals use to coerce users into downloading a malicious application. The malicious file could be hidden in banner advertisements, pop-up advertisements, or links on websites.
- A computer infected by Trojan malware can also spread it to other computers. A cyber criminal turns the device into a zombie computer, which means they have remote control of it without the user knowing. Hackers can then use the zombie computer to continue sharing malware across a network of devices, known as a botnet.
- For example, a user might receive an email from someone they know, which includes an attachment that also looks legitimate. However, the attachment contains malicious code that executes and installs the Trojan on their device. The user often will not know anything untoward has occurred, as their computer may continue to work normally with no signs of it having been infected.
- The malware will reside undetected until the user takes a certain action, such as visiting a certain website or banking app. This will activate the malicious code, and the Trojan will carry out the hacker's desired action. Depending on the type of Trojan and how it was created, the malware may delete itself, return to being dormant, or remain active on the device.

TYPES OF TROJANS

- **Backdoor Trojan**: A backdoor Trojan enables an attacker to gain remote access to a computer and take control of it using a backdoor. This enables the malicious actor to do whatever they want on the device, such as deleting files, rebooting the computer, stealing data, or uploading malware. A backdoor Trojan is frequently used to create a botnet through a network of zombie computers.
- **Banker Trojan**: A banker Trojan is designed to target users' banking accounts and financial information. It attempts to steal account data for credit and debit cards, e-payment systems, and online banking systems.
- **Distributed denial-of-service (DDoS) Trojan**: These Trojan programs carry out attacks that overload a network with traffic. It will send multiple requests from a computer or a group of computers to overwhelm a target web address and cause a denial of service.
- **Downloader Trojan**: A downloader Trojan targets a computer that has already been infected by malware, then downloads and installs more malicious programs to it. This could be additional Trojans or other types of malware like adware.
- **Mailfinder Trojan**: A mailfinder Trojan aims to harvest and steal email addresses that have been stored on a computer.
- **Ransom Trojan**: Ransom Trojans seek to impair a computer's performance or block data on the device so that the user can no longer access or use it. The attacker will then hold the user or organization ransom until they pay a ransom fee to undo the device damage or unlock the affected data.
- **Spy Trojan**: Spy Trojans are designed to sit on a user's computer and spy on their activity. This includes logging their keyboard actions, taking screenshots, accessing the applications they use, and tracking login data.

LOGIC BOMBS

- A logic bomb is a malicious piece of code that's secretly inserted into a computer network, operating system, or software application. It lies dormant until a specific condition occurs.
- When this condition is met, the logic bomb is triggered.
- Unlike viruses and worms, which can infect a system on their own, a logic bomb is often inserted by someone with inside knowledge of the system — such as when a disgruntled employee embeds a logic bomb in their company's network.
- And since they're activated by a specific condition, logic bombs can go undetected for long periods of time, until they're triggered by the coded condition.
- Logic bomb attacks can be devastating. There are instances of how logic bombs have wiped the servers of major financial institutions and other organizations. Anything that can disrupt the servers of a large company or institution has the power to cause serious havoc to the organization itself and the general population it serves.

Characteristics of a logic bomb virus

- **It lies dormant for a specific amount of time**
- **Its payload is unknown until it triggers**
- **It's triggered by a certain condition**

LOGIC BOMBS

How does a logic bomb work?

- The conditions that trigger a logic bomb can be categorized as **positive** or **negative**. Logic bombs with positive triggers detonate after a condition is met, such as when you open a particular file.
- Negative triggers launch a logic bomb when a condition is *not* met, such as when the bomb isn't deactivated in time.
- Either way, when the desired conditions are achieved, the program's system of logic will order the logic bomb to go off and inflict its damage.

Logic bombs with triggers related to dates or specific times are also known as time bombs.

BOTNETS

- A botnet is a distributed network consisting of many compromised internet-connected devices, which are controlled by a centralized botmaster, and are utilized to perform synchronized tasks.
- Each infected machine is called a bot, and together their power is used to carry out various attacks.
- The botnet is a network of robots. Developers assign them to commit a malicious task. The handlers of a botnet who controls it are called the **botmaste**r They have access to thousands of devices. They gain access by injecting a Trojan horse or other malware through email, drive-by downloads, or other means.
- Once the botnet carrier enters your device, it would inform the botmaster, and the botmaster would take control of your system.
- For botnets to evolve and become more vigorous, it must connect more and more devices to its network. The more the bots, the bigger the botnet, and the more significant the impact. Take an example. If ten people hit a website simultaneously, it won't be disturbed much. However, if a thousand people hit it simultaneously, the site would get slow, and it may even crash with an increase in number. So size is vital for a botnet.

BOTNET ARCHITECTURE

For infecting more devices and controlling the bots, botnet basically uses two network architectures – **Client-Server Model** and **Peer-to-Peer**.

Client-Server Model

- In the client-server architecture of a botnet, one of the bots acts as a central server, controlling the transfer of information from other connected bots, acting as a client.
- The botmaster uses special software to establish a connection and relay information between the server and clients. This process is known as Command and Control(C&C).
- The client-server architecture is best for taking and maintaining control over the bots. Since the control is centralized, there is no confusion during the communication.
- However, it has some downsides as well. It is easy for the security team to locate and destroy the network by targeting the central bot.
- And since there is only one control point, the botnet is dead once you destroy the server. So to overcome this, botmaster use peer-to-peer architecture.

BOTNET ARCHITECTURE

Peer-to-Peer:

- Peer-to-peer architecture is more advanced and secure than the client-server model. It does not rely on a centralized command and control(C&C) server to add new bots.
- Instead, it uses a peer-to-peer(P2P) structure. In P2P architecture, each bot act as a client and server.
- Every single bot has a list of other infected devices so that they can establish a connection with them when required.
- Since there is no centralized server, it is difficult for a security team to locate the source's position and destroy it.
- Using this architecture, botnet traffic is harder to distinguish from legitimate traffic, the bots are harder to find, and the networks are harder to take down as there is no centralized power in the network.
- While a botnet's C&C server must possess a list of all the bots in its network, in a P2P model, each peer only possesses a list of its neighboring peers.

TYPES OF BOTNET ATTACKS

- Distributed Denial of Service (DDoS) attacks: It is the most common executable attack using the network of bots. In a DDOS attack, bots send unusual traffic to the targeted website server. By doing so, intended users can not access the site. The infected bot army overloads the site to such a point that the server gets crashed.If thousands of users visit a website, it will show an access denied error message. Thus, the user won't be able to complete the desired task.
- Email Spamming: By using the thousands of devices connected through a botnet, bot herders send emails to millions of people to spam their inboxes with unnecessary ads and offers.
- Cryptocurrency Mining: The processing power of thousands of computers can collectively mine cryptocurrency like Bitcoins. Users would not be able to detect that their system's RAM and other resources are in control of a botnet.
- Ad fraud: Cybercriminals can use the botnet to run fraud ad clicks by utilizing the processing power of the infected devices. The botmaster would direct all the infected machines to click on ads placed on a website. For every click, they get a small percentage of the advertising fees.
- Generating Fake Traffic: Like the fraud ad clicks, a botnet can also generate fake traffic on a third-party website. It is generally used to get unethical financial gains from website visits.

TYPES OF BOTNET ATTACKS

- **Steal Information:** A botnet can steal personal information from the infected devices and transfer those pieces of information to cybercriminals. Further, cybercriminals use this information for carrying out extortion and other illegal activities.
- **Banner and Pop-Up Ads:** Botnet bombards the infected device with intrusive banners and pop-up ads. Pop-up ads are intriguing to trick the user so that they click on them, and malicious programs can enter the system.
- **Botnet Selling and Renting:** After a botnet serves its purpose, cybercriminals can sell or rent it. Other cyber criminals use this robot network to perform notorious tasks.

ROOTKITS

- Rootkits are malicious software that gives hackers the full administrator rights of your PC.
- It helps hackers in changing or altering the system settings or files the way an administrator could do. It creates a backdoor for other users to log in and provides full access to the system.
- The rootkit is derived from two words Root and Kit. The **Root** is referred to as a full access user account in the Unix based operating systems. While the **Kit** word represents as a collection of tools. Meaning a collection of tools to access the root account.

TYPES OF ROOTKITS

- **Hardware or firmware rootkit:** The name of this type of rootkit comes from where it is installed on your computer. This type of malware could infect your computer's hard drive or its system BIOS, the software that is installed on a small memory chip in your computer's motherboard. It can even infect your router. Hackers can use these rootkits to intercept data written on the disk.
- **Bootloader rootkit:** Your computer's bootloader is an important tool. It loads your computer's operating system when you turn the machine on. A bootloader toolkit, then, attacks this system, replacing your computer's legitimate bootloader with a hacked one. This means that this rootkit is activated even before your computer's operating system turns on.
- **Memory rootkit:** This type of rootkit hides in your computer's RAM, or Random Access Memory. These rootkits will carry out harmful activities in the background. The good news? These rootkits have a short lifespan. They only live in your computer's RAM and will disappear once you reboot your system — though sometimes further work is required to get rid of them.

TYPES OF ROOTKITS

- **Application rootkit:** Application rootkits replace standard files in your computer with rootkit files. They might also change the way standard applications work. These rootkits might infect programs such as Word, Paint, or Notepad. Every time you run these programs, you will give hackers access to your computer. The challenge here is that the infected programs will still run normally, making it difficult for users to detect the rootkit.
- **Kernel mode rootkits:** These rootkits target the core of your computer's operating system. Cybercriminals can use these to change how your operating system functions. They just need to add their own code to it. This can give them easy access to your computer and make it easy for them to steal your personal information.

TYPES OF DETECTION MECHANISMS

- **Behavioral Analysis:** In this method, the behavior of programs are analyzed, and if they take actions like rootkits, they are detected. The action depicts when there is a change in system files, differences in the timing and frequency of API calls, or considering the overall CPU utilization.
- **Signature Analysis:**Antivirus analyses the signature of the programs and detects the rootkits if its signature matches from the database. This strategy is beneficial catching known and well-published rootkits but won't work in case if the rootkit is new and custom made.
- **Difference Analysis:** In this method, the difference in the data returned by an API is calculated. It checks the difference between trusted raw data and tainted content.When you open a file, the contents you see are matched to what is actually stored on HDD. If there is a difference between the two, it indicates presence of rootkit.
- **Integrity Checking:** This method checks the system files for modifications since the installation. A cryptographic hash function can be used to create the fingerprint at the installation time, and it helps to know when a system change occurs. The fingerprint should be recreated in case of a system update.
- **Booting on Different Medium:** This method of detection is reliable in case of kernel rootkits that gets loads up before the operating system loads. It is done by booting from a different medium and then analyzing the storage for rootkits. This method works excellent because rootkits couldn't hide if it is not running,.

PHISHING

- Phishing is an attack in which the threat actor poses as a trusted person or organization to trick potential victims into sharing sensitive information or sending them money.
- As with real fishing, there's more than one way to reel in a victim: Email phishing, smishing, and vishing are three common types.

How the attack works:

- The phisher begins by **determining who their targeted victims will be** (whether at an organization or individual level) and creates strategies to collect data they can use to attack.
- Next, the phisher will create **methods like fake emails or phony web pages to send messages** that lure data from their victims.
- Phishers then send messages that appear **trustworthy** to the victims and begin the attack.
- Once the attack has been deployed, phishers will **monitor and collect the data** that victims provide on the fake web pages.
- Finally, phishers use the collected data to make illegal purchases or **commit fraudulent acts**..

TYPES OF PHISHING ATTACKS

- **Email phishing**
  The most common form of phishing, this type of attack uses tactics like phony hyperlinks to lure email recipients into sharing their personal information. Attackers often masquerade as a large account provider like Microsoft or Google, or even a coworker.
- **Spear phishing**
  Where most phishing attacks cast a wide net, spear phishing targets specific individuals by exploiting information gathered through research into their jobs and social lives. These attacks are highly customized, making them particularly effective at bypassing basic cybersecurity.
- **Smishing**
  A combination of the words “SMS” and “phishing,” smishing involves sending text messages disguised as trustworthy communications from businesses like Amazon or FedEx. People are particularly vulnerable to SMS scams, as text messages are delivered in plain text and come across as more personal.
- **Vishing**
  In vishing campaigns, attackers in fraudulent call centers attempt to trick people into providing sensitive information over the phone. In many cases, these scams use social engineering to dupe victims into installing malware onto their devices in the form of an app.
- **Whaling**
  When bad actors target a “big fish” like a business executive or celebrity, it’s called whaling. These scammers often conduct considerable research into their targets to find an opportune moment to steal login credentials or other sensitive information. If you have a lot to lose, whaling attackers have a lot to gain.

KEYLOGGING

- Keylogging, also known as keystroke logging, is the act of recording a user's keyboard interactions and device activity.
- Though it can be performed legally, it's also a form of data monitoring that hackers and identity thieves use to acquire people's personal information.
- A keylogger (or keystroke logger) is a type of software or hardware used to track and record what someone types on their keyboard. Keyloggers can be used legally and you may have even used a computer with software installed to log keystrokes for monitoring and ensuring safe or approved use.
- But what keylogging means for everyday users is very different from what it means for cybercriminals. Malicious actors can also use them to capture your personal and financial information, PIN codes and account numbers, credit card numbers, usernames, passwords, and other sensitive data — all of which can be used to commit fraud or identity theft.
-

TYPES OF KEYLOGGERS

Software-based keyloggers: Many software-based keyloggers have rootkit functionality, meaning they're able to hide in your system. Some of them are also able to track everything from information copied to your clipboard to location data and can even tap your microphone and camera.

Kernel level: These are complex and difficult to write, so they aren't especially common. Once installed, keyloggers affecting your device at the core of its operating system are especially difficult to diagnose and eradicate, as they've essentially been handed the "keys" to your device.

- **Application programming interface (API) level**: The most common form of keylogger software intercepts signals sent from your keyboard to the program a user is typing into. Think of it like a recording device waiting between your physical keyboard and a program on your computer screen, like a word processor or browser.
- **Screen level**: Known as "screen scrapers," these types of keyloggers take regular screenshots, recording what appears on the user's screen.
- **Browser level**: This is the least complex and least deeply rooted of the four types, but it can still be quite dangerous. This "form-grabbing" ploy records what you type into webforms, which may include everything from Social Security numbers to contact information to login credentials.

TYPES OF KEYLOGGERS

Hardware-based keyloggers: These keystroke loggers have a physical component to their implementation, either in the wiring or hardware of a device or in the setting around it. A common example of a hardware-based keylogger is the keyboard overlay on an ATM. Every time a bank customer presses the buttons on the criminal's fake keypad — thinking it's the legitimate ATM keypad — the keylogger records the keystrokes and forwards the information to the cybercriminal. These keyloggers can't be detected by antivirus software because they aren't installed on the computer, and they use their own internal memory to store and encrypt data. There are several general types of hardware-based keystroke loggers that range in their sophistication:

- **Keyboard**: These keyloggers are installed either in the wiring connecting a keyboard to a computer or directly in the keyboard itself.
- **Physical drive**: Keylog Trojans in this category are typically delivered via a USB drive or Mini PCI card.
- **Third-party recording**: The least sophisticated form of keylogger attack is an external recording device like a camera, which can be strategically placed to monitor public keypads or computer keyboards.

TRAPDOOR

- A computer trapdoor, also known as a back door, provides a secret -- or at least undocumented -- method of gaining access to an application, operating system or online service.
- Programmers typically don't create and retain trapdoors with malicious intent.
- They leave them in place for legitimate testing or debugging purposes, or to give service technicians emergency access to a system.
- Weaknesses in design logic also can introduce trapdoors into program code inadvertently and innocently.
- Many software developers include undocumented trapdoor passwords, which they use for maintenance or unspecified purposes.
- Malware can install trapdoor programs on Internet-connected computers.
- Once in place, trapdoor programs open an Internet port, enabling anonymous, malicious data collection or computer control from anywhere in the world.
- Combined in networks called botnets, infected computers with open ports can facilitate identity theft and other fraudulent activities without their owners' knowledge or consent.

Distributed Denial Of Service

- DDoS stands for Distributed Denial of Service. This type of attack involves sending large amounts of traffic from multiple sources to a service or website, intending to overwhelm it.
- Distributed Denial of Service, which is a malicious network attack that involves hackers forcing numerous Internet-connected devices to send network communication requests to one specific service or website with the intention of overwhelming it with false traffic or requests.
- This has the effect of tying up all available resources to deal with these requests, and crashing the web server or distracting it enough that normal users cannot create a connection between their systems and the server.
- DoS stands for Denial of Service. The difference between DoS and DDoS attacks is whether one computer is used in the attack, or the attack is sent from multiple sources.

Distributed Denial Of Service

- DDoS attacks are carried out with networks of Internet-connected machines.
- These networks consist of computers and other devices (such as IoT devices)which have been infected with malware, allowing them to be controlled remotely by an attacker. These individual devices are referred to as bots (or zombies), and a group of bots is called a botnet.
- Once a botnet has been established, the attacker is able to direct an attack by sending remote instructions to each bot.
- When a victim's server or network is targeted by the botnet, each bot sends requests to the target's IP address, potentially causing the server or network to become overwhelmed, resulting in a denial-of-service to normal traffic.
- Because each bot is a legitimate Internet device, separating the attack traffic from normal traffic can be difficult.

Zombies

- In computing, a zombie is a computer connected to a network that has been compromised by a hacker, a virus or a Trojan. It can be used remotely for malicious tasks.
- Most owners of zombie computers **d**o not realize that their system is being used in this way, hence the comparison with the living dead.
- Zombies are frequently used in denial-of-service attacks (DDoS), which refers to the saturation of websites with a multitude of computers accessing at the same time. As so many users are making requests at the same time to the server hosting the Web page, the server crashes, denying access to genuine users.
- A variant of this type of saturation is known as degradation-of-service attack and uses 'pulsing zombies': degradation of the service by periodically saturating the websites at a low intensity, with the intention of slowing down, instead of blocking, the targeted website.
- Whenever a computer gets affected by malicious software then that computer can be controlled by the attacker sitting at some different location and the owner won’t know about this.

Types of Zombies

1. Botnet Zombies: These are the compromised devices or computers that are controlled by Central Command and Control(C&C) servers by infecting computers with malware. These devices form a network called botnets. These botnets allow the criminal to coordinate for various cybercrime such as Distributing spam or DDOS.
2. Fileless Zombies: The problem with traditional malware is that they leave traces on the affected systems. Fileless Zombie operates in memory and it almost leaves no trail on the hard drive. These zombies are mostly undetectable from the traditional antivirus software making them hard to identify and mitigate.
3. IoT Zombies: Many IOT devices such as smart homes medical devices or industrial devices can be compromised and converted into zombies. These infected devices are a way to launch a big attack or can be the entry point into a big network
4. Ransomware Zombies: Some malware encrypts the victim's file, blocks those files in the victim's computer itself, and demands money to decrypt those files. This type of attack is said to be a ransomware attack. These attacks can become a zombie controlled by a ransomware controller.
5. Social Engineering Zombies: These zombies are not devices or computers they refer to individuals who manipulate others to give sensitive information by using social engineering tactics. Attackers use techniques such as fake websites, phone calls, or phishing emails to manipulate people into providing sensitive information or making them install malware by themselves.