Malware, its Types and Tips to Counter

Dilpreet Singh Bajwa

Malware:

"Malware" is combination of two words: "Malicious" + "Software" that is malware is a malicious software which has some bad intent to harm or compromise confidentiality, integrity and availability of victim's computer system, network, data, applications or operating system.

Malware consists of code which is designed to gain unauthorized access to a network or system to cause extensive damage like: disruption of services and system working, manipulation of results, stealing information etc. Malware is a broad term and it constitutes all types of malicious software like Virus, Trojan, Worm, Adware, Ransomware, Backdoor etc.

Malwares can enter in to our system through pen-drives, email attachments, spam emails, malicious links we clicked over internet and files/softwares we downloaded from the internet. Malware can also be installed by exploiting a known vulnerability in an operating system, application software or network device however generally installed due to some action by user such as clicking an malicious link.

Malware usually have following objectives but are not limited to:

- Steal, encrypt or delete private or confidential information.
- Corrupt the system.
- To provide unauthorized access of the machine or network to an attacker whenever required.
- Disrupt the services or functioning of the system.
- Compromise Security.
- Manipulation/modification of Data/Results.
- To take remote control of the system.

- To provide an opportunity to an attacker for making money.
- Capture the network traffic.
- To show unwanted advertisement and redirection to some unwanted site.
- To perform various types of attacks like DDOS, Man-in-the middle etc.
- To make a system zombie agent as part of botnet network.

Most Popular Types of Malwares:

Virus: It is the most common type of malware. Virus attaches their malicious code to other files in the system to infect them. When this infected file executed by the user or some system process then the virus also get executes and when execute, it tries to replicate itself by infecting other executable files. It requires interaction for execution and propagation i.e once a virus enters in to your system, it remains inactive until the infected program or host file is executed either by user or some other system program. Virus has the capability to infect other files, corrupt the files, disrupt and manipulate the system, stealing of confidential data or passwords etc.

Worm: Worm is also a malware and has all the capability similar to virus. The main difference between a virus and worm is that, a worm can propagate and execute independently i.e it has more capability and does not require any human interaction to replicate in order to spread to other computers over a network. Worms are independent files and generally use networks to spread itself while viruses spread to different systems through executable files. Worms generally consume bandwidth, delete or corrupt files, send emails etc.

Trojan: Trojan or Trojan horse is also a malicious program which shows no sign of its presence by not corrupting or distrupting the system. It is named after the Greek wooden horse used to conquer Troy. It appears to be a legitimate program but has some hidden/malicious functioning. Its main purpose is to capture all your activities, steal data or username/passwords and send all this information to its control server silently when connected to internet. It can also spread other malwares such as viruses and can also create backdoors to provide unauthorized access to attacker in to the system. Trojan spreads through malicious links user clicked over internet and files/software downloaded from the internet.

Adware: Adware is an unwanted program that is integrated in to some software (particularly within browsers) and its main purpose is to pop up advertisement and redirect user to some commercial site. It generates revenue for its developers by either displaying the advertisement or through "pay per click" basis if user clicks on the advertisement. It is not always malicious in

nature but compromise your system security to pop up advertisement which in turn also provides opportunity for other malwares to enter.

Spyware: Spyware is software designed to spy on someone without its knowledge i.e it gathers all information regarding any person or organization without their consent and knowledge and pass it on this information time to time to some other entity like an attacker. It monitors what user type, what user surf online, what sites a user visits, username/passwords a user have entered, credit card details and so on. Keylogger is also a type of spyware.

Ransomware: Ransomware is a malicious program that locks your system and encrypts all your files then in return wants you to pay ransom online through some crypto-currency like bitcoin in order to unlock your system and decrypt your files. If the user unable to pay the ransom then keys will not be provided to unlock/decrypt the data or all user data can be deleted. There is also not any guarantee that after paying the amount the user gets data back. For cyber criminals its very lucrative option to generate the revenue without any risk because the payment done through cryptocurrency is very difficult to trace. Ransomware code is easily available online and used by criminals to target individual users as well as big organization to earn large monetary benefits.

Backdoor: Backdoor refers to the secret hole that attackers or hackers used to gain unauthorized access to the system by bypassing its security or authentication mechanism. Some backdoors are also undocumented legitimate points of access keeps in the software by original vendors or developers for troubleshooting, maintenance, updation or for remote administration but some are installed by attackers in systems by compromising its security through virus, worm or Trojan. Backdoors provides continued access of systems to the attackers once it has been compromised and allows attackers to access the system remotely or to install other malwares.

Rootkit: Rootkits are the malicious programs used by attackers to gain administrative or root access of the system which provides full control over the system. Rootkits are designed to hide itself from user, security mechanism and even from operating system. Rootkits hide themselves by hooking and modifying API calls of operating system. Attackers used rootkits to maintain control over compromised system without user's knowledge and it provides them the ability to remotely control and execute files, access log and other files, change system settings or configuration and spy on all activities of user.

Zombie/Bot: "Bot" is derived from the word "robot" and refers to an automated program that can take full control of the compromised system when required and works as per instructions received from the command and control server or attacker. Bots in general is an automation of

some task that otherwise be handled manually like monitoring network, gathering information or providing services. Bots are automated programs that can be used for both good or bad purposes. A malicious bot is a malware having capability of self propagation, can take full control of system and can pursue attacks such as DOS towards a specific target on receiving instructions from their command and control center. Other than this bots can also sniff network packets, monitor keystrokes, gather information like usernames/passwords, credit card and other banking details and can also open backdoor on the compromised system. Bots always have tendency to remain hidden. Network of bots is called as botnet.

Symptoms that point towards malware infection in your system:

- System gets slow or crashes without any reason.
- Not be able to access internet or speed gets very slow without any apparent reason.
- The System takes a long time to open a file or folder.
- The System takes a long time to boot and shutdown.
- Advertisements pop-up, windows pop-up without any initiation from you.
- You are directed towards unwanted websites while surfing internet.
- Your friends circle receives emails that are not sent by you.
- Application running slowly or takes time to open or close down.
- Applications opening and closing automatically.
- System configuration settings changes by itself.
- Suspicious piece of software or functionality automatically downloads.
- Storage space gets occupied without any reason.
- Your antivirus disabled or its settings changed.
- Suspicious shortcuts, unwanted files and folders appear at different locations in your system.
- Internet traffic or consumption increases tremendously.

Tips to prevent your system from malware:

- Activate firewall on your system.
- Install a good Antivirus, Antimalware and internet protection programs.
- Always use long (atleast 12 characters) and complicated passwords having alphanumeric, special, lower, uppercase characters. Must ensure that for different logins different passwords can be used.

- Always update and patch up your operating system and other application software with latest updates.
- Always download software from their official websites.
- Avoid using USB drives in any public place computer system, computer labs or infected systems.
- Adhere to visit trusted and secure (https) websites.
- Do not click on suspicious links.
- Do not open suspicious or spam emails.
