MALWARE

The internet is now an efficient network for distribution of malware by attackers. It is always available, fast, and is connected to by very many people all over the globe. Malware has the ability to infect, manipulate, and destroy computing devices and networks. Some types of malwares are stealthy such that victims will not know when their devices are infected or when malware is actively causing damage to them. With the increased adoption of the internet, the increase of active computing devices and significant improvements in technology, the frequency, and sophistication of malware attacks have increased. Malware attacks currently pose a threat not only to internet security but also the internet economy. Unfortunately, the efforts to fight malware proliferation have not been so successful. The biggest challenge is with users. Internet users, knowing that some are quite new or elderly, are oblivious to the means through which malware are being transmitted. They are therefore easily becoming victims. There is also technology that makes it easier for malware to be attached in files or to be automatically downloaded onto devices when certain sites are visited. Very effective malware have become listed on dark net sites. In 2017, there was an interesting listing of malware that could be used to make ATM machines to spit out all the cash in them. Similarly, powerful malware are being sold in black markets on the anonymous deep web. With challenges in knowledge and understanding of malware, it is hard for malware to be fought. Even though different vendors of antivirus systems are putting efforts in improving the effectiveness of their programs in preventing malware, malware infections have remained the most serious threats to computers globally. Even though millions of signatures get added to antivirus knowledge bases, the attackers are even craftier. It is estimated that there are over 60 million new pieces of malware released each year. Malware creators are accessing more techniques that can produce different variants of malware that can circumvent security systems. There are those that can circumvent detections, others that can obfuscate their activities, and others that are being engineered to break through encryption. This chapter does an in-depth discussion of malware and their effects.

This chapter will discuss more about malware and will do so in the following topics:

1. Malware and its classification

2. Purpose of malware

3. Criminal business model of malware

4. Malware analysis

5. Detection techniques, etc.

CLASSIFICATION OF MALWARE

Programs that are classified as malware are essentially malicious programs that can cause damage or disruption to computers and their networks. Generally, there are three categories which include viruses, worms, and Trojans. There are, however, other types of programs that fall into this category, and they include some hacking tools and virus code constructors. The following is a comprehensive listing of the classes of malware

VIRUSES

These are malicious programs with the capability of replicating themselves using the resources of the devices that they invest. Viruses can take control of a victim's computer. As such, it can manipulate, steal, or delete data contained therein. It can also monitor browsers to capture and steal the passwords used by a user to log into online accounts such as banks and emails. Viruses can harvest a lot of sensitive information from a victim's computer. Computer viruses are also used to recruit devices into botnets by making them zombies that can send spam emails and illegitimate traffic for the purpose of performing denial-of-service (DoS) attacks. There is a particularly different type of virus that is renowned for its stubbornness called Rootkit virus. A rootkit virus is a malware that is capable of installing itself stealthily and is quite challenging to find or remove. It runs on a computer with elevated privileges and can, therefore, circumvent normal detection mechanisms such as antivirus program scans. Some antivirus programs have been added a functionality to do boot-time scans to help find and eliminate such stubborn malware. Operating systems are also receiving updates to make it more challenging for malware to get root privileges or for them to start up with the OS before security programs are even started. Viruses are somewhat easy to contain their spread when compared to worms. This is because they do not normally use networks to propagate themselves to other computers in a network. Instead, they use a rather linear method of movement to reach remote computers. This is done in three ways. The first one is where the virus infects files located on network drives. Therefore, when other computers access and download that file, it comes with the virus. The second way is whereby a virus infects a removable storage media. When such media are inserted into another computer, the virus will be able to move to the

device. Lastly, viruses can be propagated if they infect a file that is sent as an attachment to another device. When the attachment is downloaded and opened, the virus will infect the computer

Worms

Worms are malicious programs that can easily and quickly propagate themselves to infect very many computers in a short period of time.They are also notorious for employing nefarious techniques to ensure that they reach to as many computers as possible such as sending themselves through emails to one's entire contact list. This is done without the knowledge of the user. The following is a deeper categorization of worms to help tell the different types that exist.

Instant Messaging Worm

This is a type of worm that spreads itself over instant messaging (IM) systems. This type of worm infects other computers by sending links to one's contacts on these messaging platforms. The link sent to these users will automatically download the worm and infect the IM user's computer. When it infects the user's computer, it will repeat the same process where it goes through one's contact list and sends the link to other users.

Email Worms

These are specifically propagated through emails. The worms will send themselves as attachments in emails to one's contacts in an email. The worm will activate itself either when the attachment is downloaded or opened by the recipient. Email worms come coded with methods to help them propagate over emails. Some use MS Outlook services since it is a popularly used client program by enterprises for emailing needs. Other worms use either Windows MAPI (Messaging Application Programming Interface) or their own SMTP (Simple Mail Transfer Protocol) server connections to get into a messaging platform and send themselves to other users. Email worms are crafty at finding the emails of the recipients that they target They can read address books in Microsoft Outlook, read text files stored on hard disks with email addresses, or read email addresses in inbox folders

P2P Worm

It is a type of worm that is spread over peer-to-peer file-sharing networks. The worm propagates itself in a simple manner, it just copies itself to the files on the

networked computers. When a peer connects to an infected computer, the files downloaded will have the worm which will infect the downloading device

Net Worm

It is a type of worm that only propagates itself through computer networks. This is a feature that is only present in this type of worm.The malware will search for vulnerabilities in programs being run on networked computers and use the vulnerabilities to attack the hosts. For an infection to happen, the worm will send an exploit in a packet to the hosts and these packets will contain part of the worm's code that is responsible for penetrating the target computer and activating.In other scenarios, the code will have instructions to request for the download and execution of a file that contains the main attack module. Network worms can spread very fast since they maintain their presence on the network hunting for any vulnerable devices.

Trojans

Trojan horses infect a computer through the guise of a program that users will singly download. These types of malwares are known for performing actions without the authorization of users. they can initiate the deleting, blocking, modifying, or copying of data and the disruption of computer performance. However, unlike worms and viruses, they do not have the capability to replicate themselves. There are subclasses of worms based on their behaviors.

Backdoors

These are Trojans that create a secret back entry into a system or software. This backdoor access gives the attacker the power to remotely control a victim's machine. Such Trojans run their operations covertly and invisibly since they do not obtain the consent of a user. Backdoors can be used by attackers to steal data, delete files, log activities, or change the privileges of system users.

Exploit

These are malicious programs that have executable codes that can take advantage of vulnerabilities in programs running on local or remote computers. These types of malwares are used in much larger attacks where they compromise a system or soft ware, thus allowing for other malicious software or codes to be executed. Exploits are mostly used for penetration purposes into systems where other attacks will be carried out. There is a particularly unique type of exploit malware that is used to send requests to computers that will cause them to crash.

Rootkit

Trojans classified as rootkits are as evasive as rootkit viruses. They are able to hide their presence on computers and from antivirus software thereby making it hard for them to be detected. These Trojans can over a long period steal saved passwords, capture credentials, or be used to manage the victim computer during the distributed denial-of-service (DDoS) attack where the victim is one of the participants in a botnet of zombie computers. The rootkit additionally gives attackers backdoor functions that allow them to further install other malware or control the machine remotely.