Malware

What is Malware?

The term "**Malware**" refers to **MALICIOUS SOFTWARE** meaning software used to compromise computers, steal data, bypass access controls and inflict damage to the computers. Malwares is created by hackers in order to steal information from the infected machines and the stolen information will be sold in the Dark web. Malwares crafted by hackers consist of various types depending on the functionality and objective to be achieved. (Regan, 2019)

Types of Malware

Figure 1 below displays the type of Malware.

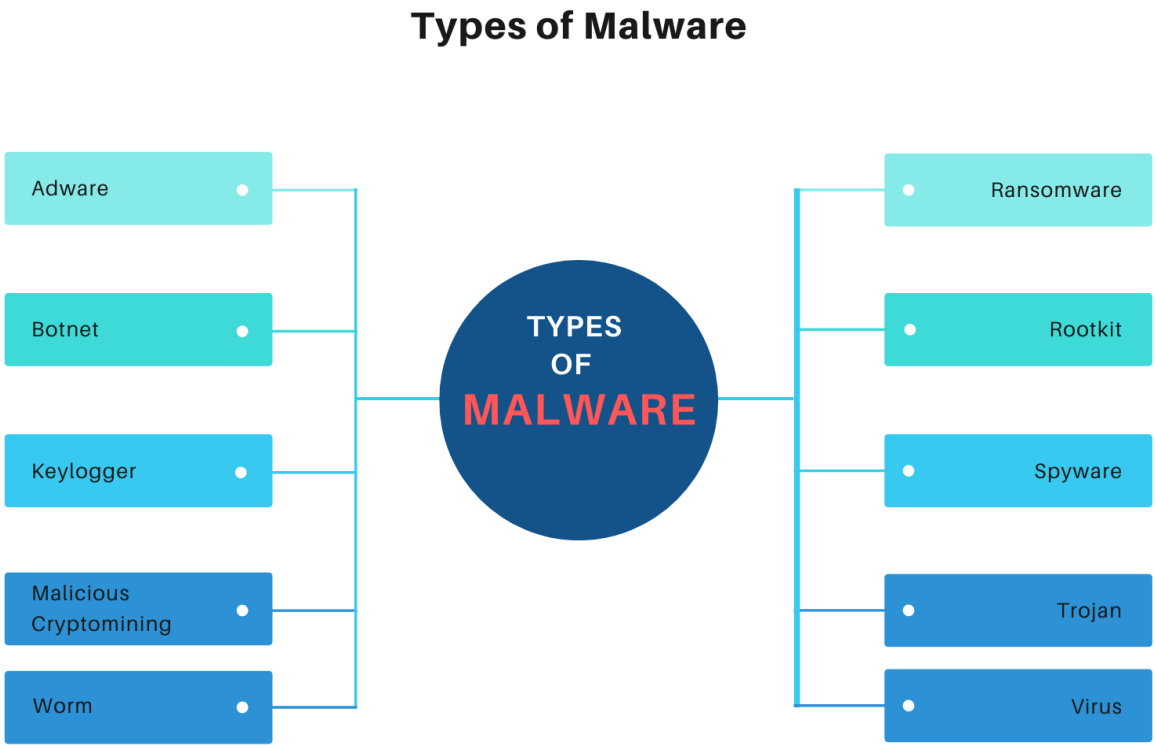

Figure 1: Types of Malware

Table 1 below describes the types of Malware and the functionalities.

Name	Description
Adware	Malware that displays advertisements through pop-up ads on websites or software. (Regan, 2019)
Botnet	Botnets refers to a collection of computers controlled by hackers for DDoS attacks. (Regan, 2019)
Keylogger	A malware that records a user's keystrokes on the keyboard. This malware's main objective is to store the collected information and send it to the attacker who searches for sensitive information such as username, passwords and banking details. (Malwarebytes, 2020)
Malicious Cryptomining	A malware is also known as drive-by mining or cryptojacking. This malware is typically installed by a Trojan and it enables the attacker to utilize the victim's machine to mine cryptocurrency such as Bitcoin or Monero. Next, cryptomining malware sends the cryptocurrency earned through the victim's machine back to the attacker. (Malwarebytes, 2020)
Worm	Computer worms spread over computer networks by exploiting the operating system vulnerabilities. Worms causes network speed to slow down and overload web servers; it can also contain payloads to perform functions to render the computer completely compromised. Worms are different compared to viruses as it does not rely on human activities to start spreading. (Regan, 2019)
Ransomware	A form of malware that encrypts all data on a computer and demands a ransom from the victim.
Rootkit	A malware that enables the attacker to gain administrator privileges on the infected machine. This malware is designed to stay hidden from the user, other softwares such as antivirus programs and the operating system itself. (Malwarebytes, 2020)
Spyware	A malware that spies on user's activities through collecting keystrokes, data harvesting and more. (Regan, 2019)
Trojan	Trojan horse disguises itself as a normal file and provides hackers remote access to an infected computer. (Regan, 2019)

Virus	A malware that can copy itself and spread to other computers. Virus is able to spread to other computers by attaching to various applications and executes the code when the user launches the infected programs. (Regan, 2019)

Figure 2: Type of Malware.

Symptoms of Malware Infection

Malware infection in a compromised system can be identified through the system displaying suspicious behaviours.

- The computer system is slow in starting or running due to the malware reducing the speed of the operating system and taking up system resources in the background.
- A large of number of pop-up advertisement is displayed on the screen is a sign of malware infection.
- The computer system crashes, freezes or displays a BSOD (Blue Screen of Death) frequently.
- Hard disk space decreases due to bloated malware which resides in the hard drive.
- Web browser's homepage is modified without user's permission and links contained within the new page leads the user to a malicious website.
- Antivirus software that is installed in the computer system cease functioning resulting the in the computer system being vulnerable to malware infection.
- All files in the system are encrypted and the user is unable to gain access to files and admin function unless a ransom is paid through cryptocurrency. This is a sign of infection caused by a ransomware.
- Malware can be hidden in the computer system and does not perform any actions that will raise suspicions. The reason is that the malware could be stealing sensitive files and recording keyboard strokes from the user or using the compromised system to spread to other computers.

(Malwarebytes, 2020)

Steps to Prevent Malware Infection

There are various steps to prevent a computer system from being infected with Malware through employing various methods:

- All users have to install antivirus software to detect malwares and prevent the malware's infection from escalating.
- Do not trust strangers online. Many hackers employ "**Social Engineering**" techniques such as sending spam emails, malicious links, fake social media profiles and fake advertisement links to the victim's email or through social media chats.
- Ensure all files or programs are downloaded from trusted official websites as files downloaded from pirating sites typically contain malware that will infect the computer system.
- Ad blockers is one of the methods advised by AVG to prevent the user from clicking potentially infected banner or pop-up ads that may infect the user's device.
- Companies and users have to create and employ a policy of browsing safe and reputable sites. The reason is to reduce the risk of the user encountering malware and being downloaded into the user's device.
- Companies have to design good policies such as monitoring network, email, web request and other activities in order to detect suspicious activities due to a malware and prevent it from spreading to other network or systems.

((Regan, 2019), (Malwarebytes, 2020), (Forcepoint, 2020))

Bibliography

DuPaul, N. (12 October , 2012). *Common Malware Types: Cybersecurity 101*. Retrieved 11 February, 2020, from VERACODE: https://www.veracode.com/blog/2012/10/common-malware-types-cybersecurity-101

Forcepoint. (2020). *What is Malware?* Retrieved 11 February, 2020, from Forcepoint: https://www.forcepoint.com/cyber-edu/malware

Malwarebytes. (2020). *All about malware*. Retrieved 11 February, 2020, from Malwarebytes: https://www.malwarebytes.com/malware/

Regan, J. (11 July, 2019). *What is Malware? How Malware*. Retrieved 11 February, 2020, from AVG: https://www.avg.com/en/signal/what-is-malware