Malware

Malware, or malicious software, is any program or file that is harmful to a computer user. Types of malware can include computer viruses, worms, Trojan horses and spyware. These malicious programs can perform a variety of functions such as stealing, encrypting or deleting sensitive data, altering or hijacking core computing functions and monitoring users computer activity.

A malware attack is a common cyberattack where malware (normally malicious software) executes unauthorized actions on the victim's system. The malicious software encompasses many specific types of attacks such as ransomware, spyware, command and control, and more.

Malware and Types of Malware

- **Virus :** A virus is the most common type of malware that can execute itself and spread by infecting other programs or files. It only works on Human Interaction. Example: CryptoLocker.
- **Worm:** A worm can self-replicate without a host program and typically spreads without any human interaction or directives from the malware authors. Example: Stuxnet
- **Trojan:** A Trojan horse is designed to appear as a legitimate software program to gain access to a system. Once activated following installation, Trojans can execute their malicious functions. It opens backdoor for other malware. Example: Emotet
- **Spyware:** Spyware is made to collect information and data on the device and user, as well as observe the user's activity without their knowledge. Example: DarkHotel,
- **Ransomeware:** Ransomware is designed to infect a user's system and encrypt its data. Cybercriminals then demand a ransom payment from the victim in exchange for decrypting the system's data. Example: RobbinHood,
- **Adware :** Adware is used to track a user's browser and download history with the intent to display pop-up or banner advertisements that lure the user into making a purchase. Example: Fireball
- **KeyLoggers:** Keyloggers, also called system monitors, are used to track nearly everything a user does on their computer. This includes emails, opened webpages, programs and keystrokes. Example: Olympic Vision

Fileless Malware Attack

- Fileless malware is a type of malicious software that uses legitimate programs to infect a computer. It does not rely on files and leaves no footprint, making it challenging to detect and remove.
- Fileless malware sneaks in without using traditional executable files as a first level of attack. Rather than using malicious software or downloads of executable files as its primary entry point onto corporate networks, fileless malware often hides in memory or other difficult-to-detect locations.
- Uses living-off-the-land techniques
- Fileless malware leverages trusted, legitimate processes running on the operating system to perform malicious activities.
- Fileless malware run on RAM (memory-based) and doesn't have any trace on the Disk (file based). This makes it impossible for a traditional antivirus which rely on signatures to detect a malware.

Mitigations:

1. Use EDR tools to monitor and detect suspicious activities.

2. Disable command line shell scripting language, including PowerShell and Window Management instrumentation,

   wherever it 's not needed