Malware is a term that's used to describe a range of different software that's developed to do a malicious action, this action can be harming a computer, gathering information, providing unauthorized access, etc.

Ransomware

- This is a type of malware that takes over a computer and demands a ransom (usually money in the form of crypto currency)
- There are different types of Ransomware like crypto malware which encrypts the files of the system until the ransom is paid
- One of the most effective defenses against Ransomware is having an effective backup system that stores files in a different location
- Another defense is having a strong antivirus/anti-malware
- As for the response for a Ransomware some organizations pay the ransom. However, this might not solve the issue as the advisory might just take the money and leave the files encrypted, in some incidents advisories even asked for more money after getting paid the initial requested amount
- As for the second method is trying to decrypt the encrypted files using the different available decryption tools

Trojan Horses

- Trojan Horses are a type of malware that disguise itself in an another legitimate software
- To Protect against this malware it's advised not to download software from unknown sources
- To validate the hash of the software.
- To have a strong anti-malware

Worms

- Worms are a type of malware that spread on its own in the network making it a dangerous type of malware
- Worms can spread using different methods, for example spreading through vulnerable services or through email attachments, network file shares, etc.
- To protect against worms it's recommended to have a strong antivirus

Rootkits

- They are a type of malware that is specifically design to allow an adversary to access the system through a backdoor
- Many rootkits have the ability to hide themselves by various techniques like hiding infecting the startup code in the master boot record (MBR) or hiding under the file system drive to make sure that users can't see it
- They are methods or tools that provide access that bypasses normal authentication and authorization procedures

Backdoor

- They can be software or hardware based
- Usually included in Trojans and Rootkits
- Sometimes used by software and hardware manufacturers to provide ongoing access to systems and software. However, there is the concern that an attacker might discover that backdoor and use it to gain access
- Detection of a backdoor can sometimes be done by checking for unexpected open port and services, but more sophisticated tools may leverage existing services.

Bots

- Bots are remotely controlled systems or devices that have a malware infection
- Groups of bots are known as botnets which are used by attackers who control them to perform various actions
- Large botnets may have hundreds of thousands of bots, most of them, and some have had millions of bots in total.
- Internet Relay Chat (IRC) was frequently used to manage client server botnets in the past, but many modern botnets rely on secure HTTP (HTTPS) traffic to help hide C&C traffic and to prevent it from easily being monitored and analyzed
- Many botnets use fast flux DNS, which uses many IP addresses that are used to answer queries for one or more fully qualified DNS names.
  - Taking down the domain name is the best way to defeat a fast flux DNS-based botnet or malware, but not every DNS registrar is helpful when a complaint is made.
- More advanced techniques also perform similar rapid changes to the DNS server for the DNS zone making it harder to take the network down.
- Command and control (C&C) servers are the core of a botnet. They allow attackers to manage the botnet, and advanced C&C tools have a broad range of capabilities that can help attackers hide their tracks, run distributed denial-of-service attacks on a massive scale, deploy and update additional malware capabilities, and respond to attempts by defenders to protect their networks.
  - C&C usually operates in a client server model where the bots are controlled through a central server

  - peer-to peer botnet control model is also used sometimes, the advantage it has over a client server model is that this model makes it harder to take down a single central server
- Detecting Bots
  - Techniques like that can be defeated in controlled networks by forcing DNS requests to organizationally controlled DNS servers rather than allowing outbound DNS requests
  - Logging all DNS requests can also provide useful information when malware hunting, because machine-generated DNS entries can frequently be easily spotted in logs
  - Analysis of bot traffic using network monitoring tools like IPSs and IDSs and other network traffic analysis systems.
  - Additional data is gathered through reverse engineering and analysis of malware infections associated with the bot
  - The underlying malware can be detected using antivirus and antimalware tools, as well as tools like endpoint detection and response tools

Keyloggers

- They are programs that capture keystrokes from keyboards, keytoggle applications may also capture other input like mouse movement, touchscreen inputs, or credit card swipes from attached devices.
- Keyloggers work in a multitude of ways, ranging from tools that capture data from the kernel, to APIs or scripts, or even directly from memory.
- Mitigation/Defense Techniques
  - Preventing software keylogging typically focuses on normal security best practices to ensure that malware containing a keylogger is not installed.
  - The use of multifactor authentication (MFA) can help limit the impact of a keylogger, even if it cannot defeat the keylogger itself.

Viruses

- Computer viruses are malicious programs that self copy and self replicate
- Viruses are typically paired with some form of search capability to find new places to spread to.
- Viruses also typically have both a trigger, which sets the conditions for when the payload will be delivered, and a payload, which is what the virus does, delivers, or the actions it performs.
- Some Types
  - Memory-resident viruses, which remain in memory while the system of device is running
  - Non-memory resident viruses, which execute, spread, and then shutdown
  - Boot sector viruses, which reside inside the boot sector of a drive or storage media
  - Macro viruses, which use macros or code inside word processing software or other tools to spread
  - Email viruses, which spread via email either as attachments or as part of the email itself using flaws within email clients

Fileless Viruses

- They spread via methods like spam email and malicious websites, and they exploit flaws in browser plug-ins and web browsers themselves.
- Once they successfully find a way into a system, they inject themselves into memory and then begin their malicious activity, including adding the ability to reinfect the system by the same process at reboot through a registry entry or other technique.
- At no point do they require local file storage because they remain memory-resident, which makes them fileless. In actuality, the—in fact, the only stored artifacts—many fileless attacks would be the artifacts of their persistence techniques
- Mitigation/Defense Techniques
  - Fileless attacks require a vulnerability to succeed, so ensuring that browsers, plug ins, and other software that might be exploited by attackers are up to date and protected can prevent most attacks.
  - Using antimalware tools that can detect unexpected behavior from scripting tools can also help stop fileless viruses.
  - Network level defenses like IPSs, as well as reputation based protection systems, can prevent potentially vulnerable systems from browsing known malicious sites.

Spyware

- Spyware is malware that is designed to obtain information about an individual, organization, or system.
- Spyware is associated with identity theft and fraud, advertising and redirection of traffic, digital rights management (DRM) monitoring, and with stalkerware, a type of spyware used to illicitly monitor partners in relationships.
- Mitigation/Defense Techniques
  - Spyware is most frequently combated using antimalware tools.
  - User awareness can help prevent the installation of spyware.

Malicious Code

- Scripts and custom built code that isn't malware can both be used by malicious actors as well.
- These attacks can happen locally or remotely via a network connection, and they often leverage built in tools like Windows PowerShell and Visual Basic, or Bash and Python on Linux systems.
- Microsoft Office macros written in Visual Basic for Applications (VBA) are another target for attackers
- Macro embedded in Office documents and similar functionality in other applications are potential targets for attackers.
- Macro attacks are no longer as common as they once were.
- Mitigation/Defense Techniques
  - Defenses against PowerShell attacks include using Constrained Language Mode, which limits sensitive commands in PowerShell.
  - Using Windows Defenders built in Antimalware Scanning Interface (AMSI) to validate scripts and to limit which modules and plug ins can be run.
  - It is also a good idea to turn on logging for PowerShell as well as Windows command-line auditing.
  - For Macros attacks, Microsoft Office disabled macros by default. This means that the primary defense is educating users to not enable macros on unknown or untrusted documents, and to provide appropriate scanning of any Office documents that are received by the organization via email or other means.

Potentially Unwanted Programs (PUPs)

- Preventing use of built in or preexisting tools like programming languages and shells can be difficult because they are an important part of how users interact with and use the systems.
  - This is why security that prevents attackers from gaining access to the systems is of the most important layers of defense
- Potentially unwanted programs (PUPs) are programs that may not be wanted by the user but are not as dangerous as other types of malware.
- PUPs are typically installed without the user's awareness or as part of a software bundle or other installation.
- Potentially unwanted programs can be detected and removed by most antivirus and antimalware programs.
- Organizations may limit user rights to install software, configure security software or to limit which software can be installed to prevent installation of PUPs and other unwanted applications on their organizationally owned PCs.

Logic Bombs

- Logic Bombs are functions or code that are placed inside other programs that will activate when set conditions are met.
- Some malware uses this type of code to activate when a specific date or set of conditions is met.

Adversarial Artificial Intelligence

- It's a developing field where artificial intelligence (AI) is used by attackers for malicious purposes.
- Every new technology provides attackers with a new attack surface, and ML is no different.
- The focus of adversarial artificial intelligence is
  - Data poisoning
  - Security and analytic AI and ML algorithms with adversarial input that serves the attacker's purposes, or attacks against privacy.
- Helpful Steps
  - Understand the quality and security of source data.
  - Work with AI and ML developers to ensure that they are working in secure environments and that data sources, models, and tools are maintained in a secure manner.
  - Ensure that changes to AI and ML algorithms are reviewed, tested, and documented.
  - Encourage reviews to prevent intentional or unintentional bias in algorithms.
  - Engage domain experts wherever possible.
- Artificial Intelligence, which focuses on accomplishing "smart" tasks by combining ML, deep learning, and related techniques that are intended to emulate human intelligence
- Machine Learning, which is a subset of AI, ML systems modify themselves as they evolve to become better at the task that they are set to accomplish.