WHAT IS MALWARE?

Malware is short for malicious software, meaning software that can be used to compromise computer functions, steal data, bypass access controls, or otherwise cause harm to the host computer. Malware is a broad term that refers to a variety of malicious programs. Most common types of malware; adware, bots, bugs, rootkits, spyware, Trojan horses, viruses, and worms.

ADWARE

Adware (short for advertising-supported software) is a type of malware that automatically delivers advertisements. Common examples of adware include pop-up ads on websites and advertisements that are displayed by software. The advertisements may be in the user interface of the software or on a screen presented to the user during the installation process.

RANSOMWARE

Ransomware is a form of malware that essentially holds a computer system captive while demanding a ransom. The malware restricts user access to the computer either by encrypting files on the hard drive or locking down the system and displaying messages that are intended to force the user to pay the malware creator to remove the restrictions and regain access to their computer. Ransomware typically spreads like a normal computer worm ending up on a computer via a downloaded file or through some other vulnerability in a network service.

ROOTKIT

A rootkit is a type of malicious software designed to remotely access or control a computer without being detected by users or security programs. Once a rootkit has been installed it is possible for the malicious party behind the rootkit to remotely execute files, access/steal information, modify system configurations, alter software (especially any security software that could detect the rootkit), install concealed malware, or control the computer.

Rootkit prevention, detection, and removal can be difficult due to their stealthy operation. Because a rootkit continually hides its presence, typical security products are not effective in detecting and removing rootkits. As a result, rootkit detection relies on manual methods such as monitoring computer behavior for irregular activity and signature scanning.

Organizations and users can protect themselves from rootkits by regularly patching vulnerabilities in software, applications, and operating systems, updating virus definitions, avoiding suspicious downloads, and performing static analysis scans.

SPYWARE

Spyware is a type of malware that functions by spying on user activity without their knowledge. These spying capabilities can include activity monitoring, collecting keystrokes, data harvesting (account information, logins, financial data), and more. Spyware often has additional capabilities as well, ranging from modifying security settings of software or browsers to interfering with network connections.

TROJAN HORSE

A Trojan horse, commonly known as a "Trojan," is a type of malware that disguises itself as a normal file or program to trick users into downloading and installing malware. A Trojan can give a malicious party remote access to an infected computer. Once an attacker has access to an infected computer, it is possible for the attacker to steal data (logins, financial data, and even electronic money), install more malware, modify files, monitor user activity (screen watching, keylogging, etc.)

VIRUS

A virus is a form of malware that is capable of copying itself and spreading to other computers. Viruses often spread to other computers by attaching themselves to various programs and executing code when a user launches one of those infected programs. Viruses can also spread through files, documents. Viruses can be used to steal information, harm host computers and networks, steal money, render advertisements, and more.

WORMS

Computer worms are among the most common types of malware. They spread over computer networks by exploiting operating system vulnerabilities. Worms typically cause harm to their host networks by consuming bandwidth and overloading web servers. Computer worms can also contain "payloads" that damage host computers. Payloads are pieces of code written to perform actions on affected computers beyond simply spreading the worm. Payloads are commonly designed to steal data, delete files, and modify files.

Computer worms can be classified as a type of computer virus, but there are several characteristics that distinguish computer worms from regular viruses. A major difference is that computer worms have the ability to self-replicate and spread independently while viruses rely on human activity to spread (running a program, opening a file, etc.). One example would be for a worm to send a copy of itself to everyone listed in your e-mail address book. Then, the worm replicates and sends itself out to everyone listed in each of the receiver's address book.

MALWARE PREVENTION AND REMOVAL

There are several general best practices that organizations and individual users should follow to prevent malware infections. Some malware cases require special prevention and treatment methods, but following these recommendations will greatly increase a user's protection from a wide range of malware:

- Install and run anti-malware and firewall software. When selecting software, choose a program that offers tools for detecting, quarantining, and removing multiple types of malware. At the minimum, anti-malware software should protect against viruses, spyware, adware, Trojans, and worms. The combination of anti-malware software and a firewall will ensure that all incoming and existing data gets scanned for malware and that malware can be safely removed once detected.

- Keep software and operating systems up to date with current vulnerability patches. These patches are often released to patch bugs or other security flaws that could be exploited by attackers.

- Be vigilant when downloading files, programs, attachments, etc. Downloads that seem strange or are from an unfamiliar source often contain malware.

ANTI-VIRUS

Anti-virus software is a program or set of programs that are designed to prevent, search for, detect, and remove software viruses, and other malicious software like worms, Trojans, and more. These tools are critical for users to have installed and up-to-date because a computer without anti-virus software installed will be infected within minutes of connecting to the internet.

There are several different companies that build and offer anti-virus software and what each offers can vary but all perform some basic functions:

- Scan specific files or directories for any malware or known malicious patterns

- Allow you to schedule scans to automatically run for you

- Allow you to initiate a scan of a specific file or of your computer, or of a CD or flash drive at any time.

- Remove any malicious code detected –sometimes you will be notified of an infection and asked if you want to clean the file, other programs will automatically do this behind the scenes.

- Show you the 'health' of your computer

ANTI-SPYWARE

Anti-spyware software detects spyware through rules-based methods or based on downloaded definition files that identify common spyware programs. Anti-spyware software can be used to find and remove spyware that has already been installed on the user's computer, or it can act much like an anti-virus program by providing real-time protection and preventing spyware from being downloaded in the first place.

Most modern-day security suites bundle anti-spyware functionality alongside anti-virus protection, personal firewalls, etc.

POP-UP BLOCKER

A pop-up blocker refers to any software or application that disables any pop-up advertisement window that you would see while using a Web browser. Some pop-up blockers may try to close all pop-up windows, some may remove all advertising from a publisher's Web site, and still others may help you choose which pop-up windows you want to be closed with block list feature.

ACCESS CONTROL LIST

It can be used as a medium of security, operates at server level to ensure that certain activities from users and websites can be restricted on a computer system. Unauthorized access can be stopped. The ACL can be configured and changed as needed to stop and allow access to the computer system.

Access Control List (ACL) are filters that enable you to control which routing updates or packets are permitted or denied in or out of a network. They are specifically used by network administrators to filter traffic and to provide extra security for their networks. This can be applied on routers.