Explanation About Virus,Worms,Spyware,Ransomware,Rootkit,Adware and Trojan

NAME :- CHARCHIT SUBEDI

DATE :- 2022/FEB/9

TIME : 12:20 PM

CONTENT **PAGE NO.**

Introduction to Virus

A computer virus is a type of computer program that, when executed, replicates itself by modifying other computer programs and inserting its own code. If this replication succeeds, the affected areas are said to be "infected" with a computer virus.

Computer viruses generally require a host program. The virus writes its own code into the host program. When the program runs, the written virus program is executed first, causing infection and damage. A computer worm does not need a host program, as it is an independent program or code chunk. Therefore, it is not restricted by the host program, but can run independently and actively carry out attacks.

Virus writers use social engineering deceptions and exploit detailed knowledge of security vulnerabilities to initially infect systems and to spread the virus. The vast majority of viruses target systems running Microsoft Windows, employing a variety of mechanisms to infect new hosts, and often using complex anti-detection/stealth strategies to evade antivirus software. Motives for creating viruses can include seeking profit (e.g., with ransomware), desire to send a political message, personal amusement, to demonstrate that a vulnerability exists in software, for damage and denial of service, or simply because they wish to explore cybersecurity issues, artificial life and evolutionary algorithms.

Computer viruses cause billions of dollars' worth of economic damage each year.

In response, an industry of antivirus software has cropped up, selling or freely distributing virus protection to users of various operating systems.

What is a Boot Sector Virus?

A boot sector virus is a type of virus that infects the boot sector of floppy disks or the Master Boot Record (MBR) of hard disks (some infect the boot sector of the hard disk instead of the MBR). The infected code runs when the system is booted from an infected disk, but once loaded it will infect other floppy disks when accessed in the infected computer. While boot sector viruses infect at a BIOS level, they use DOS commands to spread to other floppy disks. For this reason, they started to fade from the scene after the appearance of Windows 95 (which made little use of DOS instructions). Today, there are programs known as 'bootkits' that write their code to the MBR as a means of loading early in the boot process and then concealing the actions of malware running under Windows. However, they are not designed to infect removable media.

The only absolute criteria for a boot sector is that it must contain 0x55 and 0xAA as its last two bytes. If this signature is not present or is corrupted, the computer may display an error message and refuse to boot. Problems with the sector may be due to physical drive corruption or the presence of a boot sector virus.

How to remove boot sector virus

Removing a boot sector virus can be difficult because it may encrypt the boot sector. In many cases, users may not even be aware they have been infected with a virus until they run an antivirus protection program or malware scan. As a result, it is critical for users to rely on continually updated virus protection programs that have a large registry of boot viruses and the data needed to safely remove them. If the virus cannot be removed due to encryption or excessive damage to existing code, the hard drive may need reformatting to eliminate the infection.

What is file Virus ?

A File Virus is a notorious computer malware that can easily intrude your PC and infect your files. This perilous threat is a nasty file encrypting virus created by hackers to thug money from users. It is mainly intended to hijack your files and extort ransom fees. This brutal computer infection can easily alter your system without permission and hide deep into your system. It will start endless malevolent actions that can downgrade your system performance. File Virus will lock all your files and change their extension. It will make your files inaccessible and show error message when you try to open your files. This perilous threat will demand ransom fees to unlock your files. It will also leave ransom note on your computer screen to explain the decryption and payment method.

File Virus will change the default desktop wallpaper with its ransom image. This notorious threat will give you some time to pay the money through BitCoin. It also threats users to pay the money before given time otherwise their files will get removed completely. It is deceptive malware infection that you can never trust. It will not unlock your files after getting the money.File Virus will keep bothering you to pay ransom fees and until you pay money your computer will be locked and useless. Many of users get cheated and didn’t got their files even after paying the ransom money. You should act smart and remove this threat to recover your data safely by using any data recovery software. It is the only or your can best method to solve this problem.

What is a macro virus?

A macro virus is a computer virus written in the same macro language used to create software programs such as Microsoft Excel or Word. It centers on software applications and does not depend on the operating system (OS). As a result, it can infect any computer running any kind of OS, including Windows, macOS and Linux.

Macro viruses work by adding their code to the macros associated with documents, spreadsheets and other data files. They target software rather than systems and can infect any OS. Macro viruses have been around since 1995 when the Concept virus first appeared. It was accidentally included on a CD-ROM (compact disc read-only memory) called Microsoft Compatibility Test and shipped by Microsoft to hundreds of corporations. With the release of Microsoft Office 2000 and all subsequent versions, Microsoft disabled macros by default. Since then, it's become more difficult for bad actors to easily launch macro viruses. However, as long as macros are available to users, the risk of macro viruses remains serious.

In fact, if a macro virus infects a file, it can potentially damage not only the document itself, but the system and other applications. So, security teams should not ignore the risk.

How does macro viruses spread ?

- when files are shared over a network
- when infected files are placed on a removable disk and shared among multiple users
- when an infected file is downloaded via a modem and opened

- when an infected file is downloaded via the internet or intranet and opened

How are macro viruses removed?

If a system is infected with a macro virus, it's critical to remove it as soon as possible with specific security software tools for macro virus detection and removal. This can stop it from spreading across the network.The first step in removing macro malware is to reboot the infected computer in safe mode. Deleting temporary files can speed up virus scanning, free up disk space and remove any malware-infected temp files. It's also recommended to run a virus scan on the infected computer. If a real-time antivirus program is already running on the machine, an on-demand virus scanner can be used to check for undetected malware. In this scenario, the on-demand scanner is used first, followed by a full scan using real-time antivirus. This should detect and quarantine any macro malware found on the system.

What is Cluster Virus ?

A type of computer virus that associates itself with the execution of programs by modifying directory table entries to ensure the virus itself will start when any program on the computer system is started. If infected with a cluster virus it will appear as if every program on the computer system is infected; however, a cluster virus is only in one place on the system.

What is a Stealth Virus?

A stealth virus is a kind of malware that does everything to avoid detection by antivirus or antimalware. It can hide in legitimate files, boot sectors, and partitions without alerting the system or user about its presence. Once inside a computer, a stealth virus allows an attacker to take over the functions of the infected computer.

How to Protect Yourself from Stealth Virus

You can detect the virus by starting the system via a disk boot to avoid systems the virus has control over and then beginning an antivirus scan. However, even if detected here, there is a chance the virus has copied itself into another file on the system, so it remains a challenging virus to fully eradicate. In general, the best countermeasure is to use strong antivirus software designed to detect viruses and their hidden counter parts.

1. **SPYWARE :-** Spyware is software with malicious behavior that aims to gather information about a person or organization and send it to another entity in a way that harms the user. For example, by violating their privacy or endangering their device's security. This behavior may be present in malware as well as in legitimate software. Websites may engage in spyware behaviors like web tracking. Hardware devices may also be affected. Spyware is frequently associated with advertising and involves many of the same issues. Because these behaviors are so common, and can have non-harmful uses, providing a precise definition of spyware is a difficult task.

TYPES OF SPYWARE

There are four common types of spyware. Their function ranges from tracking your browser activity so marketers can target your interests, for instance, to monitoring your keystrokes and nearly everything you do on your device. Here are some of the unique tactics each type of spyware uses to track you:

- Adware tracks your browser history and downloads with the intent of predicting what products or services you’re interested in. It's used for marketing purposes.·
- Trojans are a type of malware disguised as legitimate software. Just like the Trojan horse from Greek mythology, a trojan tricks you into letting it in (or, more specifically, onto your device), by acting like a software update or file. Then it damages, disrupts, or steals your data.
- Internet tracking is a common practice used to follow your web activities—like browsing history and downloads—mostly for marketing purposes.

System monitors are a type of spyware that can capture just about everything you do on your computer. System monitors can record all of your keystrokes, emails, chat room dialogs, websites visited, and programs run. System monitors are often disguised as freeware.

How to recognize spyware

How do you get spyware? Well, it was once more of a problem for Windows operating systems, but that's no longer strictly the case. Spyware can affect PCs, Macs, and iOS, or Android devices, including mobile phones and tablets. Basically, if your device can connect to the internet, it can be infected with spyware.

Some common ways your device might become infected with spyware include:

- Accepting a prompt or pop-up without reading it first
- Downloading software from an unreliable source
- Opening email attachments from unknown senders
- Pirating media such as movies, music, or games
- Clicking a link to a malware-laden website

Spyware creators may use clever tricks to deceive you. The spyware may be packaged alongside free software made to seem like a useful tool, or in an email attachment that seems legitimate.

How to remove spyware

Spyware is a common problem for internet users. If you think your device has been infected, there are steps you can take to remedy the problem.

i. Run a scan with your security software: The scan will help to identify and remove malware.
ii. Download and run a virus removal tool: A reputable virus removal tool scans for threats that traditional antivirus software may not detect.
iii. Uninstall apps you don't recognize: Go to your phone's settings, click on "Apps," and uninstall any apps you find suspicious.
iv. Run an antivirus or malware scan: You may have an app that came packaged with your phone, or you may need to download and install a reputable app from the official app store for your device.

What to do after spyware removal.

Your work isn't quite finished once the spyware has been removed from your device. There are some steps you should take to protect your personal data from being further exposed.

- Change your passwords: Once your system has been cleaned, take steps to secure your personal data by changing your email and other important account passwords.
- Alert your financial institutions: If you believe financial credentials such as credit card data may have been exposed, make sure your financial institution is on the lookout for fraudulent activity and keep an eye out yourself.

2. **RANSOMWARE :-** Ransomware is a type of malicious software (malware) that threatens to publish or blocks access to data or a computer system, usually by

encrypting it, until the victim pays a ransom fee to the attacker. In many cases, the ransom demand comes with a deadline. If the victim doesn’t pay in time, the data is gone forever or the ransom increases. Ransomware attacks are all too common these days. Major companies in North America and Europe alike have fallen victim to it. Cybercriminals will attack any consumer or any business and victims come from all industries. Several government agencies, including the FBI, advise against paying the ransom to keep from encouraging the ransomware cycle, as does the No More Ransom Project. Furthermore, half of the victims who pay the ransom are likely to suffer from repeat ransomware attacks, especially if it is not cleaned from the system.

Who is At Risk of Ransomware?

Any device connected to the internet is at risk of becoming the next ransomware victim. Ransomware scans a local device and any network-connected storage, which means that a vulnerable device also makes the local network a potential victim. If the local network is a business, the ransomware could encrypt important documents and system files that could halt services and productivity.

If a device connects to the internet, it should be updated with the latest software security patches, and it should have anti-malware installed that detects and stops ransomware. Outdated operating systems such as Windows XP that are no longer maintained are at a much higher risk.

Why You Shouldn’t Pay Ransomware ?

After ransomware encrypts files, it shows a screen to the user announcing files are encrypted and the amount of money that must be paid. Usually, the victim is given a specific amount of time to pay or the ransom increases. Attackers also threaten to expose businesses and announce that they were victims of ransomware publicly.

The biggest risk of paying is never receiving cipher keys to decrypt data. The organization is out the money and still doesn’t have decryption keys. Most experts advise against paying the ransom to stop perpetuating the monetary benefits to attackers, but many organizations are left without a choice. Ransomware authors require cryptocurrency payments, so the money transfer cannot be reversed.

RANSOMWARE PREVENTION AND DETECTION

Prevention for ransomware attacks typically involves setting up and testing backups as well as applying ransomware protection in security tools. Security tools such as email protection gateways are the first line of defense, while endpoints are a secondary defense. Intrusion Detection Systems (IDSs) are sometimes used to detect ransomware command-and-control to alert against a ransomware system calling out to a control server. User training is important, but user training is just one of several layers of defense to protect against ransomware, and it comes into play after the delivery of ransomware via an email phish.A fallback measure, in case other ransomware preventative defenses fail, is to stockpile Bitcoin. This is more prevalent where immediate harm could impact customers or users at the affected firm. Hospitals and the hospitality industry are at particular risk of ransomware, as patients' lives could be affected or people could be locked in or out of facilities.

HOW TO REMOVE RANSOMWARE

Call federal and local law enforcement: Just as someone would call a federal agency for a kidnapping, organizations need to call the same bureau for ransomware. Their forensic technicians can ensure systems aren't compromised in other ways, gather information to better protect organizations going forward and try to find the attackers.

3. **ROOTKIT :-** The name "rootkit" derives from Unix and Linux operating systems, where the most privileged account admin is called the "root". The applications which allow unauthorized root or admin-level access to the device are known as the "kit".

A rootkit is software used by cybercriminals to gain control over a target computer or network. Rootkits can sometimes appear as a single piece of software but are often made up of a collection of tools that allow hackers administrator-level control over the target device.

Types of rootkits