MCSE 568

Malware

Malware, Virus & Spyware

"Malware" is short for "malicious software" - computer programs designed to infiltrate and damage computers without the users consent. "Malware" is the general term covering all the different types of threats to your computer safety such as viruses, spyware, worms, trojans, rootkits and so on.

These malicious programs can perform a variety of functions, including stealing, encrypting or deleting sensitive data, altering or hijacking core computing functions and monitoring users' computer activity without their permission.

(Types of Malware)

Virus | Worms | Trojan | Ransomware | Spyware | Adware

Malware, Virus & Spyware

WHAT IS VIRUS ?

Virus is a program or Software.

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

Affected Files

Document or Text files.

Image files.

Videos files.

Audio files.

Vital
Information
Resources
Under
Seize.

First PC Virus: ALK ClONER

- Affects the boot floppy disk
- found in 1982
- OS was DOS 3.3
- Apple II

```
Elk Cloner:
The program with a personality

    It will get on all your disks
      It will infiltrate your chips
        Yes it's Cloner!

    It will stick to you like glue
      It will modify ram too
        Send in the Cloner!
```

First Network Virus: Creeper

- Affects ARPANET
- found in 1970

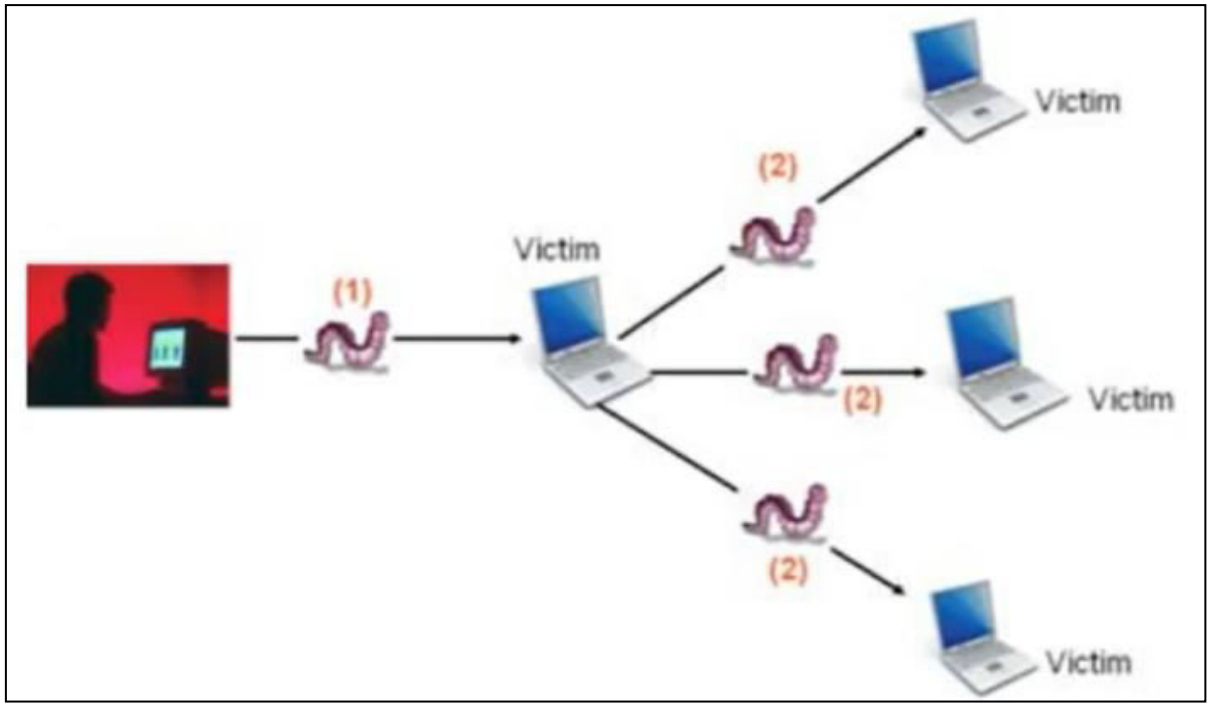
I'M THE CREEPER,
CATCH ME
IF YOU CAN

Malware, Virus & Spyware

2. Worm: A **worm** virus is a malicious, self-replicating program that can spread throughout a network without human assistance. It full the memory space.

It comes from

- Downloading
- Internet Surfing
- Email



Infect Computers in the network or slow down the network

Protect PC against Worm

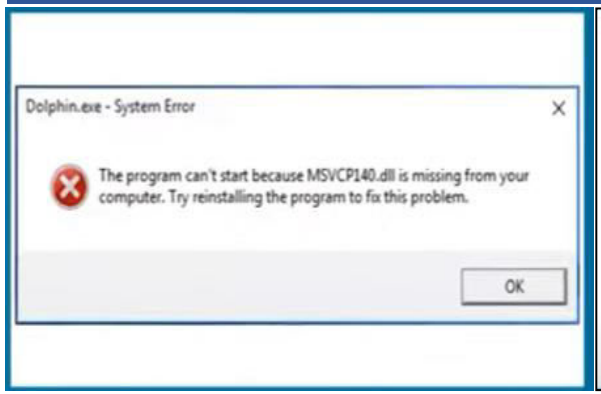
Making sure that your computer has all the latest updates installed is the best defence against worms

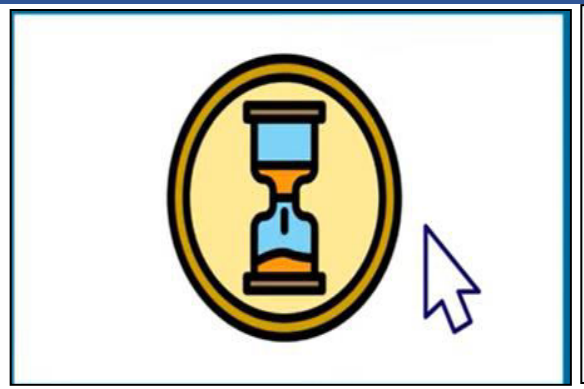
Malware, Virus & Spyware

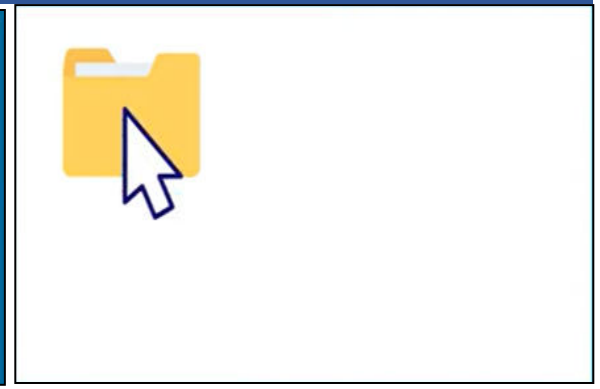
3. Trojan horse: A **Trojan horse**, or Trojan, is a type of malicious code or software that looks legitimate but can take control of your computer. A Trojan is designed to damage, disrupt, steal, or in general inflict some other harmful action on your data or network.

When you install a fake software then Trojan horse can be installed

Probable Symptom of Trojan virus





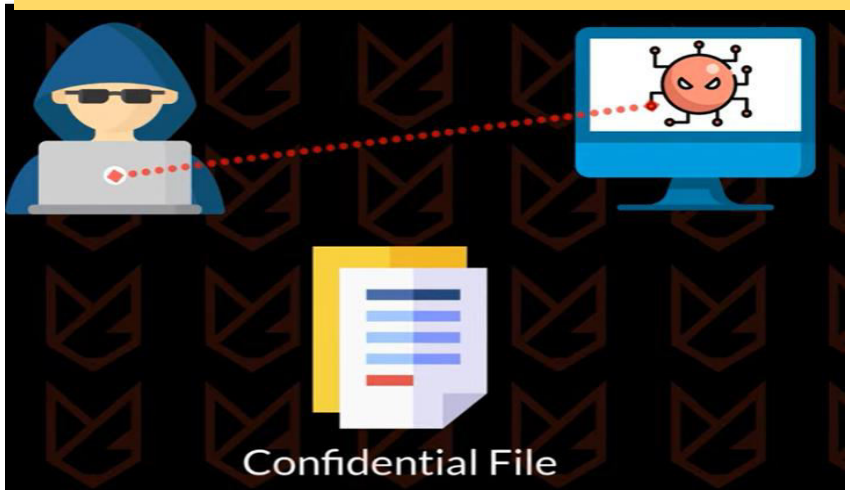


1. System Errors
2. Strange Pop-ups
3. Slow Computer
4. Strange Behavior

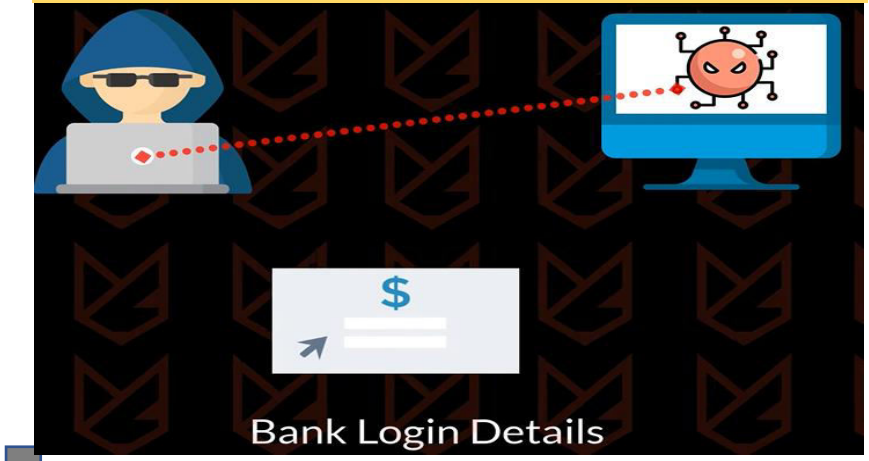
Malware, Virus & Spyware

How harmful Trojan virus is

1. Steal confidential files



2. Steal pin/password



3. Illicit Activities using hacked machine (arrest hacked user)

Malware, Virus & Spyware

How to Remove Trojan virus

1. Run MS Defender Scan
Start->MS Defender Scan>Virus & Protection->Full Scan

2. Delete Temporary Files
Start->Disk Cleanup>Select Temp Files

3. Remove System Restore Point
Start->Create Restore Point->Configure->Delete

4. Reset Browser Settings
Google Chrome Menu->Settings->Advanced->
Reset and Cleanup->Restore Default Settings

5. Scan PC with AntiMalware
Use MalwareFox to do it
https://www.malwarefox.com/

Malware, Virus & Spyware

4. Ransomware: It iss a type of malicious software that infects a computer and restricts users' access to it until a ransom is paid to unlock it. Ransomware variants have been observed for several years and often attempt to extort money from victims by displaying an on-screen alert.

How to Remove

First, identify the type of attack and file extension, the following website can help in this purpose, https://www.nomoreransom.org/en/index.html
Secondly, use the following application to decrypt infected files

AVAST: Alcatraz Decryptor, Bart Decryptor, Crypt888 Decryptor, Hidden Decryptor, Noobcrypt Decryptor and Cryptomix Decryptor

Bitdefender: Bart Decryptor CERT

Polska: Cryptomix / Cryptoshield decryptor

CheckPoint: Merry X-Mas Decryptor and BarRax Decryptor

Eleven Paths: Telefonica

Cyber Security Unit: Popcorn Decryptor.

Emsisoft: Crypton Decryptor and Damage Decryptor.

Kaspersky Lab: Updates on Rakhni and Rannoh Decryptors.

Malware, Virus & Spyware

5. Spyware: It is any software that installs itself on your computer and starts covertly monitoring your online behavior without your knowledge or permission. Spyware is a kind of malware that secretly gathers information about a person or organization and relays this data to other parties

6. Adware: It is **a form of malware that hides on your device and serves you advertisements**. Some adware also monitors your behavior online so it can target you with specific ads.

How to prevent malware

- Keep your computer and software updated. ...
- Use a non-administrator account whenever possible. ...
- Think twice before clicking links or downloading anything. ...
- Be careful about opening email attachments or images. ...
- Don't trust pop-up windows that ask you to download software. ...
- Limit your file-sharing.

See live Cyber Threat
https://threatmap.checkpoint.com/