A Comparative Study on Virus Vs Worm Vs Trojan

Sayaliambre[1], Siddharth Nanda[2], Rajeshwari Gundla[3]
[1]U.G. Student, [2]Faculty, [3]Senior Faculty
SOE, ADYPU, Lohegaon, Pune, Maharashtra, India[1]
IT, iNurture, Bengaluru, India[2,3]

Abstract **-** This survey paper mentions three kinds of malware, they're virus, worm and trojan. These malwares provide partial or full management to Associate in nursing furtive user for doing any malicious activities. Most malware needs the user to initiate its operation. During this paper the 3 kinds of malware and their sorts and what ought to the users ought to do to guard their systems kind these sorts of malware.

Keywords **-**furtive, malware and malicious.

I. INTRODUCTION

Malware [1] is any piece of package that is meant to cause hurt to our system or network. Malware is totally different from traditional programs during a manner that almost all of them have the flexibility to unfold itself within the network, stay undetectable, causes changes/damage to the infected system or network, persistence.one of the malware sort is virus which needs human intervention to run and propagate. Second sort is worm that is comparable to an endemic however doesn't need any human intervention to run and propagate within the network. The third sort is trojan, it's the malware concealment in alternative legitimate files.

II. THE PRIMARY THREE KINDS OF MALWARE

A. Virus: A virus[2]may be a tiny program written to change the manner a computer operates, while not the permission or information of the user an local must meet two criterias:

1. It should execute itself. it'll usually place its own code within the path of execution of another program.
2. It should replicate itself. for instance, it should replace alternative viable files with a duplicate of the virus infected file. Both network servers and desktop computers will be infected same by the virus.

Most of the viruses are made to enter the computer by getting undetected by deleting files damaging programs or also by reformatting the hard disk. Alternative isn't designed to try and do any harm, however merely to copy themselves and create their presence well-known by presenting text, video, and audio messages. They use erratic behaviour and also lead to system crashes. Additionally, several virus's area unit bug-ridden, and these bugs might cause system crashes and information loss. Virus's[5]area unit usually well-known for physically harming our systems.

There are five recognized kinds of viruses:

i). File infector viruses - Program files are infected by file infectors. Viable code are used by this viruses which contains .com and .exe files. The will infect alternative files once Associate in Nursing infected program is run from floppy, hard drive, or from the network. several of those virus's area unit memory resident. once memory becomes infected, any antiseptic viable that runs becomes infected. Samples of well-known file infector viruses embody Jerusalem and Cascade.

ii). Boot sector viruses - System space of a disk is infected by boot sector virus. All floppy disks and laborious disks (including disks containing solely data) contain a little program within the boot record that's run once the computer starts up. Boot sector viruses attach themselves to the current a part of the disk and activate once the user makes an attempt to begin up from the infected disk. These virus's area unit forever memory resident in nature. Most were written for DOS, but, all COMPUTERs, in spite of the OS, area unit potential targets of this sort of virus. All that's needed to become infected is to aim to begin up your computer with Associate in Nursing infected disc thenceforth, whereas the virus remains in memory, all discs that aren't write protected can become infected once the floppy disk is accessed. Samples of boot sector virus's area unit kind, Disk Killer, statue maker, and Stoned.

iii). Master boot record viruses - With the same appearance as a boot sector virus the master boot record virus infects the disk. The distinction between these 2 virus sorts is wherever the infective agent code is found. They save a appropriate copy of the master boot record with a different location. Viruses wont let Windows Ngo computer boot as they are infected by boot sector viruses or master boot sector viruses. This is often because of the distinction in however the OS accesses its boot data, as compared to Windows 95/98.

iv). Many-sided viruses - Multipartite viruses infect each boot records and program files. These area unit significantly troublesome to repair. If the boot space is clean, however the files aren't, the boot space are reinjected. identical holds true for improvement infected files. If the virus isn't off from the boot space, any files that you just have clean are reinjected.

v). Macro viruses - A macro virus is a virus which is written in the language called macro which is used for software programs and also it includes Microsoft excel. When the system is affected with macro virus it directly affects the software applications by which it causes some malicious actions automatically when that particular software is opened.

How To defend Your Systems From computer Virus? One of the most effective ways in which to guard yourself from an endemic is to grasp one thing regarding the manner they work. By learning the way to be a wise soul in your

claim, you'll be able to with success navigate around a majority of the infectious material that lurks regarding waiting to strike. the knowledge Technology cluster has provided this page, containing many sections on virus-safe computing, in order that you would possibly have the knowledge you wish to stay yourself antiseptic right at your fingertips.

B. Worm -A worm[3] has similar characteristics of an endemic. Worms also are self-replicating, however self-replicating of a worm is during a totally different manner. Worms [6] area unit stand alone and once it's infected on a computer, it searches for alternative computers connected through network (LAN) or net association. The new computer and continues to look for alternative computers on the network to copy.

Due to nature of replication through the network, a worm usually consumes a lot of system resources as well as network information measure, inflicting network servers to prevent responding.

Types of worms:

i). Email worms - Email Worms unfold through infected email messages as Associate in Nursing attachment or a link of Associate in Nursing infected web site.

ii). Instant electronic messaging worms - Instant worms unfold by causing links to the contact list of instant messaging application.

iii). Internet worms - Internet worm can scan all accessible network resources victimization native OS services and/or scan the web for vulnerable machines. If a computer is found vulnerable it'll decide to connect and gain access to them.

iv). IRC worms - Irc chat channel are unfurl by Irc worms which causes links to infected websites and causes infected files.

v). File-sharing networks worms - File-sharing network worms place a duplicate of them within the shared folder and unfold via P2P network.

How to defend Your Systems from worm? A user ought to be well-prepared all the time to handle an endemic attack because it is turning into common currently. With the correct preventative measures in situations, any malicious code won't be able to corrupt your files or harm your package programs. Ever hospitable determine the viruses that may harm your system and your information.

Topping the list is that the recommendation to take care of Associate in Nursing up-to-date OS and every one alternative package patches. This helps scale back the danger close the latterly discovered vulnerabilities.

Secondly, ne'er think about Associate in Nursing obsolete antivirus package. transfer a free antivirus package like Comodo Free Antivirus from the web and keep protected against malicious package. The Comodo Free Antivirus package offers multi-layered levels of threat and virus protection to stay your system keep one's eyes off from issues.

You should not open the mails or the attachments that arrives in it. Most of the time, hackers create use of emails because it has the flexibility to sneak into a strong arm.

Lastly, if your system has been negotiated, then you must confine, scan and repair.

C. Trojan - A Trojan[4] horse or Trojan may be a kind of malware that's usually disguised as legitimate package. Trojans is used by cyber-thieves and hackers trying to get access to users' systems. Users area unit generally tricked by some kind of social engineering into loading and corporal punishment Trojans on their systems. Trojans will send cyber criminals to keep a close eye on you, to steal your data and to gain access to your device. These actions will include:

- Deleting information
- Blocking information
- Modifying information
- Copying information
- Disrupting the performance of computers or computer networks

How Trojans will impact you? Trojans area unit classified in line with the kind of actions that they'll perform on your computer:

i). Backdoor - A backdoor Trojan provides malicious users remote over the infected computer. they allow the author to try and do something they need on the infected computer – as well as causing, receiving, launching and deleting files, displaying information and rebooting the computer. Backdoor Trojans areas do not unite a band of fatalities computers to create a botnet or zombie network that may be used for criminal activities.

ii). Exploit - Exploits area unit programs that contain information or code that takes advantage of a vulnerability among application package that's running on your computer.

iii). Rootkit - Rootkits area unit designed to hide sure objects or activities in your system. usually their main purpose is to stop malicious programs being detected – so as to increase the amount within which programs will run on Associate in Nursing infected computer.

iv). Trojan-Banker - To steel your data such as credit cards, debit card etc. Trojan banker programs have being designed for online banking.

v). Trojan-DDoS - By generating different requests – from your computer other infected computers – the attack will deluge the target address resulting in a rejection of service.

vi). Trojan-Downloader - Trojan-Downloaders will transfer and install new versions of malicious programs onto your computer – as well as Trojans and adware.

vii). Trojan-Dropper - These programs area unit utilized by hackers so as to put in Trojans and / or viruses – or to stop the detection of malicious programs. Not all antivirus programs area unit capable of scanning all of the parts within this sort of Trojan.

viii). Trojan-Fake Ab- Trojan-Fake Ab programs simulate the activity of antivirus package. they're designed to extort

cash from you – reciprocally for the detection and removal of threat even if the threats that they report are literally non-existent.

ix). Trojan-Game felon - From Online gamers the program steals the user account data.

x). Trojan-IM - Trojan-IM programs steal your logins and passwords for fast electronic messaging programs – like ICQ, MSN courier, AOL Instant courier, Yahoo electronic device, Skype and plenty of a lot of.

xi). Trojan-Ransom - This type of Trojan will modify information on your computer – in order that your computer doesn't run properly otherwise you will now not use specific information. The criminal can solely restore your computer's performance or unblock your information, once you have got paid them the cost that they demand.

xii). Trojan-SMS - If you text message from your simple device to any premium rate phone numbers then it is going to cost you money.

xiii). Trojan-Spy - Trojan-Spy programs will spy on however you're victimization your computer – for instance, by pursuit the info you enter via your keyboard, taking screen shots or obtaining an inventory of running applications.

xiv). Trojan-Mail finder - These programs will harvest email addresses from your computer.

How to defend Your Systems from Trojan? By putting in effective anti-malware package, you'll be able to defend your devices – as well as COMPUTERs, laptops, Macs, tablets and cell phones across Trojans. You can find and forestall Trojan attacks on your computer, whereas Kaspersky Mobile Security will deliver first virus protection for robot smartphones

Kaspersky laboratory has anti-malware product that defend the subsequent devices against Trojans:

- Windows COMPUTERs
- Linux computers
- Apple Macs
- Smartphones
- Tablets

III. CONCLUSION

As we've got mentioned during this paper regarding malware and its 3 sorts, therefore we should always watch out and currently we all know the way to defend our system from malware attacks.

IV. REFERENCES

[1]. https://www.avg.com/en/signal/what-is-malware [Referred on date: 8th March 2019]
[2]. https://en.wikipedia.org/wiki/Computer_virus [Referred on date: 8th March 2019]
[3]. https://searchsecurity.techtarget.com/definition/worm [Referred on date: 8th March 2019]
[4]. https://en.wikipedia.org/wiki/Trojan_horse_(computing) [Referred on date: 8th March 2019]
[5]. https://patents.google.com/patent/US5842002A/en
[6]. https://www.researchgate.net/profile/Arun_Lakhotia/publication/220178085_Analysis_and_Detection_of_Computer_Viruses_and_Worms_An_Annotated_Bibliography/links/0912f50f9cc4a10cde000000/Analysis-and-Detection-of-Computer-Viruses-and-Worms-An-Annotated-Bibliography.pdf
[7]. https://onlinelibrary.wiley.com/doi/abs/10.1046/j.1365-2648.1998.00768.x