International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 1 | ISSN : 2456-3307

Module Functioning of Computer Worm, PC Virus and Anti Virus Programs

Soumen Chakraborty

Department of Information Technology, MCKV Institute of Engineering, MAKAUT, West Bengal, India

csoumen88@gmail.com

ABSTRACT

The normal antivirus method includes detecting the virus, designing a solution, and providing and deploying the solution, in such concern, it is very difficult to hinder each machine from being compromised by way of virus. This paper suggests that to enhance new dependable antivirus program some problems have got to be solved similar to: a brand new system to observe all metamorphic virus copies, new riskless monitoring procedures to observe the brand new viruses or attaching a digital signature and a certificate to every new application.Viruses tends to propagate more slowly in addition they have extra mature defenses due to the presence of a large anti-virus enterprise that actively seeks to establish and manipulate their unfold. Unlike an epidemic laptop worms does no longer have to connect itself to an existing software. Computer worms almost and always motive damage to the community if most effective with the aid of drinking bandwidth whereas viruses quite often corrupt or regulate files on a target laptop. Laptop worms are hated when you consider that they consumes extra Bandwidth and also they could crash computer systems if they're infected with pc worms.

Keywords: Computer Worms, Boot Sectors Virus, Antivirus, Scanning, Polymorphic Viruses

I. INTRODUCTION

PC worm is a self-replicating computer application. It uses a network to send copies of itself to different nodes i.E., desktops on the network and it is going to accomplish that without any user involvement.Viruses are ought to be attached to the system documents belongs to the operating approach it requires some kind of consumer motion to support their propagation. Viruses tends to propagate more slowly in addition they have more mature defenses because of the presence of a gigantic anti-virus enterprise that actively seeks to establish and manipulate their unfold. Not like an endemic laptop worms does now not need to connect itself to an existing software. Computer worms close to and invariably cause harm to the network if only by using consuming bandwidth the place as viruses ordinarily corrupt or adjust records on a goal pc. Pc worms are hated due to the fact they consumes more Bandwidth and in addition they might crash computers if they are contaminated with computer worms. Contaminated desktops may additionally use for other assaults corresponding to DDos, phishing assaults and so forth.. Computer worms are one form of malware together with viruses and Trojans.A individual normally installs worms by inadvertently opening an email attachment or message that involves executable scripts.Once established on a laptop, worms spontaneously generate additional e-mail messages containing copies of the worm. They may additionally open TCP ports to create networks security holes for different purposes, and so they could attempt to "flood" the LAN with spurious Denial of carrier (DoS) knowledge transmissions.A pc virus is a laptop application that can reproduction itself and infect a laptop without permission or skills of the person. With a view to preclude detection through customers,some viruses employ different sorts of deception comparable to the following procedures[1] [2] :

- ✓ **Overwriting Virus**: this type of virus overwrites documents with their possess replica. Of path, it is a very primitive system, however it is obviously the simplest technique of all. Overwriting viruses

cannot be disinfected from a system.Contaminated files need to be deleted from the disk.

- ✓ **Accomplice Infection**: one process to fitting a associate to an EXE file is to provide the virus the identical base name as the detailed software, however use a .COM extension instead of .EXE. This process was employed with the aid of the Globe virus, first detected in 1992. When the victim attempts to launch an EXE program, he or she commonly types its identify with out the extension. In such cases, home windows offers precedence to a file with the .COM extension over a file with the identical base name but with the .EXE extension.
- ✓ **Appending Virus**: in this technique, a jump (JMP) guideline is inserted at the entrance of the host to factor to the end of the original host. A ordinary example of this virus is Vienna. The appender manner may also be implemented for any other form of executable file, equivalent to EXE, NE, PE, and ELF codecs, and so on. Such records have a header part that retailers the handle of the important entry point, which, quite often, will likely be changed with a new entry factor to the start of the virus code appended to the top of the file.
- ✓ **Prepending Virus**: This virus inserts its code on the front of host applications.It is a simple sort of contamination, and it is as a rule very successful. Virus writers have carried out it on more than a few operating techniques, inflicting most important virus outbreaks in lots of. An instance of a COM prepender virus is the Hungarian virus Polimer.512.A, which prepends itself, 512 bytes lengthy, at the front of the executable and shifts the usual software content material to comply with itself.
- ✓ **Cavity or Spacefiller Virus**: This virus attempts to put in itself in this empty area even as no longer dangerous the actual program itself. An skills of this is that the virus then does now not broaden the size of the program and might prevent the necessity for some stealth methods. The Lehigh virus was once an early instance of a cavity virus. Given that of the obstacle of writing this variety of virus and the confined number of feasible hosts, cavity viruses are infrequent.
- ✓ **Compressing Virus**: A precise virus infection manner makes use of the approach of compressing the content of the host application. Regularly this system is used to cover the host software's dimension expand after the infection by means of packing the host application sufficiently with a binary packing algorithm.
- ✓ **Encrypted Virus:** contains a constant decryptor, adopted by way of the encrypted. Slightly effortless to discover when you consider that decryptor is regular. The primary recognized virus that implemented encryption was once Cascade on DOS.Oligomorphic virus changes its decryptors in new generations. The easiest method to vary the decryptors is to use a set of decryptors alternatively of a single one. The first identified virus to make use of this technique used and carried a number of dozen distinctive decryptors, and the virus picked one randomly.
- ✓ **Boot Sectors Virus:** this virus takes expertise of the executable nature of master boot record (MBR) and partition boot sector (PBS). A laptop infected with a boot sector virus will execute the virus's code when the machine boots up. Michelangelo virus is an example of a Boot Sectors Virus.
- ✓ **Macro Virus:** infects a Microsoft phrase or identical application and causes a sequence of movements to be carried out automatically when the applying is started or anything else triggers it. Macro viruses tend to be stunning but fairly harmless. A ordinary influence is the undesired insertion of some comic textual content at particular points when writing a line. A macro virus is on the whole unfold as an email virus. A recognized illustration in March, 1999 used to be the Melissa virus.
- ✓ **Malicious cell code (MMC):** mobile code is a light-weight software that is downloaded from a far flung system and executed in the community with minimal or no consumer intervention. Java applets, JavaScript scripts, visible general Scripts (VBScripts), and ActiveX controls are probably the most most widespread examples of mobile code that you may stumble upon even as searching the online or reading HTML-formatted email. An attacker might use mobile code for a style of nasty movements, together with monitoring your looking movements, acquiring unauthorized access to your file approach, infecting your computer with a Trojan horse, hijacking your web browser to discuss with web sites that you didn't intend to visit, and so on.

II. METHODS AND MATERIAL

A. Antivirus Open Issues

Detection ways have some fundamental problems. First of all, they are only excellent towards identified viruses and now not superb towards evolutionary or new viruses. Secondary,they tend to take a obvious amount of time to scan a procedure or networks for the patterns. Thirdly, a scanner or its virus sample database ought to be updated very customarily to remain potent. Subsequence the next issues must be solved:

- ✓ If the virus is cleverly written to continuously stay within this typical conduct, it is also intricate to notice its presence utilising the present monitoring procedures.Can we introduce new dependable monitoring techniques to discover the brand new viruses?
- ✓ Metamorphic viruses are complicated to become aware of given that their creators have the talents of knowing the weaknesses of antivirus scanners. The boundaries of antivirus scanners come from the bounds of static and dynamic analysis systems. If we have some copies of a metamorphic virus, is there a brand new process to realize all metamorphic virus copies?
- ✓ can we use public key cryptography to remedy the pc virus obstacle? In this case the entire builders have got to embed their digital signature inside their software and they have to put together a certificates that is signed by way of a will identified certificate authority. The developers of working systems have got to present a new method to repeat, download and set up the brand new software.

B. Classification of computer Worms

Classification headquartered on conduct

- ✓ **Stealth Worms :** This worm doesn't unfold in a speedy fashion but rather they unfold in a stealthy. They're very elaborate to realize.
- ✓ **Polymorph Worms:** To make the signature founded detection extra difficult these worms can change themselves for the duration of the propagation.
- ✓ **File Worms:** These worms are modified version of viruses however unlike viruses this worms does no longer join their presence with any executable documents. They conveniently reproduction their code to some other disk or directory hoping that these new copies will in the future be accomplished via the person.
- ✓ **Multi-vector Worms:** This kind of worms use special kind of propagation approaches with a purpose to make more hosts susceptible for attack and simply propagate at the back of firewalls.
- ✓ **E-mail Worms:** email themselves to different email addresses and make the consumer execute e-mail Attachments with malicious code or use bugs in the e mail programs to get attachments carried out mechanically.

C. Evolution of Virus

Computer malwares will also be categorised according to their one of a kind traits in a couple of quite a lot of manners, equivalent to classification by way of target or classification via illness mechanism. One of these classification forms is in line with concealment methods employed [3].

Virus Obfuscation Techniques

Virus-like programs first appeared on microcomputers within the 1980s. To project virus scanning products, virus writers continually increase new obfuscation methods to make virus code more intricate to observe. To flee widely wide-spread scanning, a plague can regulate its code and alters its look on every infection. The tactics which were employed to obtain this end variety from encryption to polymorphic tactics, to state-of-the-art metamorphic approaches [4] [5].

- ✓ **Encrypted Viruses**

The easiest option to alternate the looks of a virulent disease is to use encryption. An encrypted virus consists of a small decrypting module (a decryptor) and an encrypted virus body. If one more encryption secret is used for every illness, the encrypted virus physique will look different.Ordinarily, the encryption procedure is instead easy, such as xor of the key with each byte of the virus physique. Easy xor is very practical on account that xoring the encrypted code with the important thing once more will give the normal code and so an endemic can use the same events for both encryption and decryption. With encryption, the

decryptor remains regular from new release to generation. As a result, detection is possible established on the code pattern of the decryptor. A scanner that can't decrypt or detect the virus body instantly can recognize the decryptor as a rule.

✓ **Polymorphic Viruses**

To overcome the trouble of encryption, namely the truth that the decryptor code is lengthy and distinctive adequate for detection, Polymorphic viruses can exchange their decryptors in newer generations. They can generate a tremendous number of specific decryptors which use exclusive encryption procedure to encrypt the virus physique. A polymorphic virus for that reason has no parts that keep constant on each illness. To notice polymorphic viruses, anti-virus application comprises a code emulator which emulates the decryption system and dynamically decrypts the encrypted virus body. Due to the fact all polymorphic viruses lift a consistent virus physique, detection is still feasible headquartered on the decrypted virus code.

✓ **Metamorphic Viruses**

To make viruses more resistant to emulation, virus writers developed countless developed metamorphic methods. In keeping with Muttik, "Metamorphics are bodypolymorphics". A metamorphic virus no longer best alterations it decryptor on every infection but additionally its virus physique. New virus generations look one-of-a-kind from one an extra and they do not decrypt to a consistent virus physique.

III. RESULTS AND DISCUSSION

A. Classification headquartered on scanning

Random Scanning : Random Scanning worm will generate a random IP addresses making use of a pseudorandom quantity generator. As a consequence each host on the community is equally likely to be scanned. CodeRed v2 and SQL Slammer are the random scanning worms.

Localized Scanning : Localized scanning is an easy method utilized by computer worms to search for the inclined hosts. Localized scanning trades off between the nearby and the global search of vulnerable hosts and has been used by Code red II and Nimda worms

Sequential Scanning : Sequential scanning worms' scans IP addresses sequentially. After the worm compromises a vulnerable host, it checks the host subsequent to this inclined host. Blaster worm employed sequential scanning.

Topological Scanning : Topological scanning worms rely on the local information contained within the compromised hosts to locate new targets. Nearby knowledge includes /etc/hosts file, e mail addresses and so forth. Topological scanning used to be used by Morris worm.

Hit list Scanning: The worm author gathers a list of potentially prone hosts beforehand, which might be special first when the worm is launched. This accelerates the unfold of the worm at an initial stage. Hit record scanning used to be utilized by Slammer worm.

B. Identifying an Epidemic

Frequently viruses will set off windows to show up and disappear randomly for your approach as they do their work. These shall be very rapid however may incorporate an ordinary warning or request so that you can click good enough.

Some viruses can create small information records that refill hard power house or allow applications to be downloaded to your workstation, turning your computer right into a community server for pirated records or pornography. In the event you see a unexpected scale back in free drive space, you might have a pandemic.· Viruses can corrupt or injury information documents and applications. It will cause you to lose foremost knowledge or expertise error messages and blue displays on your working approach. These may also be signs of hardware failure, even though hardware failure is much less possible on more recent techniques.

Your laptop crashes extra as a rule or generally your pc may also shutdown robotically this can also be a sign of virus assault.[6]Your keyboard doesn t work effectively or unexplained printing problems happens, may be a symptom of virus attack.

C. How Virus will get into your PC?

You obtain an epidemic with the aid of walking an infected application or opening an contaminated knowledge file. Viruses mainly infect program records, which can be identifiable with the aid of the COM or EXE software extension.Some viruses may additionally infect batch records similar to BAT and CMD records. Every so often, viruses infect information documents. Generally affected knowledge documents are Microsoft office files comparable to word doctors and Excel XLS files. MP3 documents have additionally been mentioned as possible virus sources, despite the fact that few viruses that take advantage of MP3 records exist.Viruses are unfold by way of passing documents from one user to one other. Which you can receive them through e-mail, by means of downloading files from the web, or by using sharing documents over the community or through removable storage instruments similar to floppy disks.Many viruses infect techniques should you download and set up an infected software. You can acquire the virus-contaminated file by way of downloading it from the web, opening an infected electronic mail attachment, or utilizing a file-sharing network. You don‟t constantly have to open an infected attachment from an email to receive an epidemic. Some viruses can infect early versions of Outlook by merely opening an infected
e mail.

D. Tips on how to avert Virus Attack.

Replace your operating method often. It blocks security holes that can be exploited through viruses or hackers.

Update your Anti-Virus. Don't rely on the automatic updates. Open the Anti-Virus software, assess when the final update was once performed and if necessary assess for updates manually. Make sure the program and the virus definitions are each consistently up to date.Update all software. Attempt to preserve all of your software up-to-date. Every software in this day and age has a web based connection, which can mean a gateway for adware spyware and adware and many others to get in. That is in most cases true for browsers. So make certain you have got the ultra-modern version. Do not click on links despatched to you through electronic mail by means of an unfamiliar sender as it is a fashioned means for malicious internet site to hook you in. Alternatively go to the browser and style within the web pages name in straight.

Avert unhealthy web sites like grownup web sites, piracy web sites and file sharing websites. Any internet site where you get a continuous number of pop up pages on any link you press is as a rule dangerous and will have to be refrained from. Watch out when installing applications. Consistently study any packages you want to install. Do not set up a application just seeing that it seems to fit your wants. If it's a just right software there shall be many reviews and suggestions.
Preclude Clicking Popup adverts. If you are cautious and you realize the website is reputable then it can be k, however a number of the time they're not and are to be refrained from. Certainly ones that say they are going to fortify your laptop.

Be Vigilant .In the event you get a home windows pop up that appears adore it's scanning your tough drive for viruses or blunders, but you've gotten under no circumstances obvious this application earlier than shut it immediately.

Run Virus cleanup traditionally. Most antivirus packages have a scheduler with a view to agenda a common scan of your computer. Ensure that is enabled, and examine regularly to peer if it has been run.[8]

E. Which Anti-Virus software is better?

Reliability and convenience of work - absence of anti-virus "hold ups" and different technical issues, requiring distinctive technical advantage from a user. Reliability of anti-virus applications is the predominant criterion, given that even the “absolute anti-virus" may come to be vain, if it is not in a position to finish the scanning process and hangs, leaving a component of your disks and records unchecked, thereby leaving the virus within the approach undetected.

High-quality of detection of all predominant varieties of viruses,scanning inside of document documents, spreadsheets (Microsoft word, Excel, Office97), packed and archived records. Absence of false positives. Ability to therapy contaminated objects.

Availability of anti-virus models for all of the standard platforms (DOS, All windows platform,Novell NetWare, OS/2, Alpha, Linux and so on.), not best on-

demand scanning, but additionally scanning onthe-fly capabilities, availability of server types with probability for network administration.[7]There are hundreds of thousands of antivirus products but two to be the quality: Bitdefender's and Kaspersky lab‟s.Bitdefender may be very robust on account that it's a combo of signature-founded detection, analytic detection, and conduct detection. Merchandise from avast, avira, Eset, F comfy, BullGuard, G knowledge
also perform good.[10]

IV.CONCLUSION

Laptop viruses were round virtually so long as computers. Pc viruses have dramatically improved in complexity through the years. The rationale of this survey used to be to know the consumer expertise and attitude closer to a laptop virus. Situated on the survey carried out we located that the majority of the respondents grievance about virus assault and most of them used antivirus software to look after their pc. This confirmed that individuals had been conscious in regards to the problems prompted with the aid of viruses and in addition the significance of antivirus. The viruses have a big have an impact on to the customers exceptionally once they had been unable to perform their everyday hobbies work due to viruses. We additionally concluded from the survey that male respondents had higher expertise about viruses and used antivirus software‟s than feminine respondents. We located that persons had typical competencies regarding viruses so we offered them potential about various symptoms and prevention techniques of virus assaults, the best way to comprehend that they have been attacked via virus and which is healthier antivirus program.

V. ACKNOWLEGDMENTS

I would like to specific my precise appreciation , have been a enormous value for me. I wish to thank you for encouraging my research. I'm also grateful for the assistance given by way. A distinctive thanks to my father and mother for his or her help and encouragement during my study. I would also wish to thank all of my buddies who supported me in writing, and help me to try towards my intention.

VI. REFERENCES

[1]. J. cock, Computer Viruses and Malware, Springer (2006)

[2]. E. Skoudis and L. Zeltser, Malware: Fighting Malicious Code, Prentice Hall (2003)

[3]. Peter J. Denning, editor. Computers Under Attack: Intruders, Worms and Viruses. ACMPress (Addison-Wesley), 1990.

[4]. Christopher V. Feudo. The Computer VirusDesk Reference. Business One Irwin, Homewood, IL, 1992.

[5]. Harold Joseph Highland, editor. Computer Virus Handbook. Elsevier Advanced Technology, 1990.

[6]. Computer Viruses: How to Avoid Infection http://www.msubillings.edu/cotfaculty/security/al viruses.pdf pg 1-6)

[7]. Behavioral And Performance Analysis Model For Malware Detection Techniques A.Edwinrobert,.Dr.M.Hemalatha International Journal Of Computer Engineering & Technology (Ijcet) Issn 0976 – 6367(Print) Issn 0976 – 6375(Online)Volume 4, Issue 1, JanuaryFebruary(2013),pp.141-151

[8]. Bits & PC's 10 Step Guide to Protect Against Viruses (2012,march 4) http://www.bapcs.co.uk/10-stepguide-to-protect-against-viruses

[9]. Dancho Danchov. 20 Jul 2004. Reducing "Human Factor" Mistakes. Article in MISC Network Security.(2003,July23)(online)http://www.windowsecurity.com/articles/Reducing_Human_Factor_Mistakes.html

[10]. How Anti-virus Software Works?? Sarika Choudhary Ritika Saroha Mrs. Sonal Beniwal International Journal of Advanced Research in Computer Science and Software Engineering (Volume 3, Issue 4, April 2013 ISSN: 2277 128X pg 483-4)

[11]. AusCERT, AFP, AHTCC, NSW Police, NT Police, Queensland Police, SA Police, Tasmania Police, WA Police, Victoria Police. 2005. Computer Crime and Security Survey 2005. (online).http://www.auscert.org.au/render.html?it=2001.