Virus and Worm Control; Tips for Safer Computing

Dr.M.EEzema
Computer Science Department
University Nigeria Nsukka
modesta.ezema@unn.edu.ng
phone : 07037951472

Abstract - The internet today spans the globe and serves billions of users, providing an environment in which a single virus can conceivably cause rapid and widespread damage to systems throughout the world. Today new viruses sweep the planet in minutes and can corrupt data, slow networks down, or harm your reputation This paper work will look at different types of virus, virus detecting programs, common modes of transmission, prevention and control of viruses and worms. An overview of the major types of viruses and worms and how they function will be discussed. As the Internet expands its reach into more and more homes and viruses inevitably spread more rapidly, computer users have an increasing responsibility to be aware of these issues and their impact on the global computer community to avoid future disaster.

Index Terms : virus, spam, worm, e-mail, internet, anti-virus , computer

1 INTRODUCTION

computer viruses; [1] computer viruses are small software programs that are designed to spread from one computer to another and to interfere with computer operations. A virus might corrupt or delete data on your computer, use your e-mail program to spread itself to other computers, or even erase everything on your hard disk. Computer viruses are often spread by attachments in e-mail messages or instant messaging messages. That is why it is essential that you never open e-mail attachments unless you know who sent it and you are expecting it. [2] On the other hand Computer worms are malicious software applications designed to spread via computer networks . When you are online, you expose your vulnerability to malicious codes that have been growing in virulence and ferocity over the years. These program codes have gone beyond mere annoyances with the worst kinds disabling your personal computer, but they have become portals for remotely perpetuating more sinister activity that can clandestinely hack into sites, mount denial of services or steal confidential and personal data for fraudulent financial gain at your expense. [3] In late 1992, the number of computer viruses was estimated from 1,000 to 2,300 viruses. In 2002 there were 60,000 known viruses, Trojans, worms, and variations. Today there are well over 100,000 known computer viruses. Studies and researches show that a computer connected to the Internet may experience an attack every 39 seconds.[4] The authors (programmers) of malware are continually writing new malicious code to expose and exploit vulnerability of systems as a result of progressive growth of internet connectivity and complexity of systems. Their motives could be to infiltrate, damage or to gain unwarranted access to government confidential information resources and/or to increase the marketability of their products (anti –malware, anti-spam, antivirus) Computer virus writers use many strategies to evade detection such as space filling, compressing and encryption, on the other hand; the antivirus software tries to remove such attack when used. [5] The 2011 Norton Cybercrime Report reveals that there were 431 million global cybercrime victims who lost $388 billion in real money losses and computer time. This is a lot more compared to the estimated $288 billion in revenues from the black markets for cocaine, heroin and illegal drug trades combined. For sure, not all of these losses were incurred due to Trojans, worms, viruses, root kits and malware. But when you consider that roughly 4.3% of cybercrimes involve damages to PC resulting from online downloads of infected content over the internet, you are looking at a computed $17 billion in annual losses due to malware and virus infection. To mention but a few the activities of rough software cannot be exhausted and there is need for us to be very cautious of them.

2 TYPES OF COMPUTER VIRUSES

Every year computer experts surprise the world with their new inventions, therefore rough software programmers need to create new generations of viruses to cope with the latest computing technologies. As a result of this competition each year hundreds of new viruses are found in the world. These are grouped as follows;

2.1 File-Infecting Virus:

This class of virus attach itself to the executablefiles, which are the files ending with file extension name .exe, .com, e.t.c. , and these are the main program files and drivers. If any of them is infected the virus code will be executed during the first run by loading itself to the memory , deceiving the user by allowing the program to execute normally. When the user runs any other applications, the virus replicates itself in order

to be attached to that **application. The virus will remain undetected until when it triggers for destruction and this depends on the authors**

2.2 Boot Sector Virus:

Boot sector computer viruses are most commonly spread using physical media. An infected floppy disk or USB drive connected to a computer will transfer virus when the drive's volume boot record (VBR) is read, then modified or replace the existing boot code. When next a user tries to boot his computer, the virus will be loaded and run immediately as part of the master boot record. It's also possible for email attachments to contain boot virus code. If opened, these attachments infect the host computer and may contain instructions to send out further batches of email to a user's contact list. Improvements in basic input/output system (BIOS) architecture have reduced the spread of boot viruses by including an option to prevent any modification to the first sector of a computer's hard drive. 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..

2.3 Macro Viruses

[5] A macro virus is a computer virus written in the same macro language used for software applications like word processors. Its effect is to release a chain of events in conjunction with the application. Microsoft Word is an example of an application susceptible to macro viruses; this explains why it is a bad idea to open suspicious or unknown attachments even if they may appear legitimate. Because macro programs embedded in these documents run automatically when the document is opened, it is a likely mechanism to spread viruses. Once triggered, the macro virus can

embed itself in other documents, including any future documents created after the virus attack, as well as conceivably download software to the target computer. An example of this type of virus is the Melissa Virus from 1999; after opening the infected document from email, the targeted computer would then send itself to the first 50 email addresses in the person's contact list, thereby replicating itself quickly. Because a macro virus works using the application rather than an operating system, it can also infect non-Windows operating system computers as well. Macro viruses are also be referred to as script viruses and can also be embedded within web pages. The best defense against being infected by a macro virus, besides being very careful of what email attachments you open, is having a quality, updated antivirus program..

2.4 Script Virus:

This type of virus is written using script languages, they spread and infect files by taking advantage of vulnerabilities in the Microsoft Windows operating systems; opening e-mails or accessing Web pages which includes tainted scripts will activate the virus. This type of viruses has the ability to change its signature each time the virus is reproduced in order to remain undetected by antivirus software.

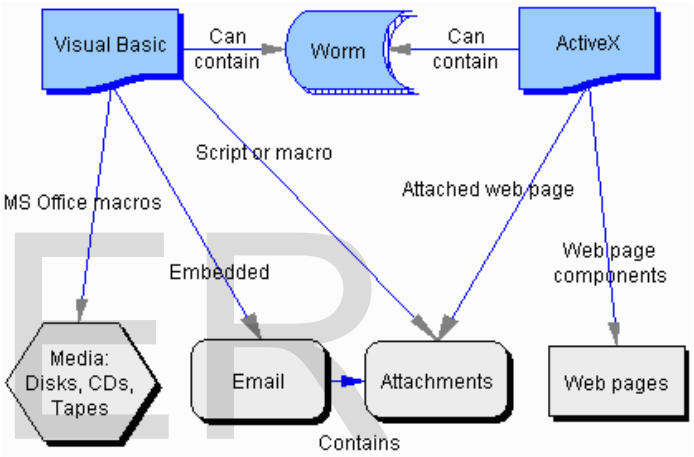

Fig. 1. Script virus infection cycle

2.4 Polymorphic Virus:

Polymorphic virus includes a scrambled virus body and a decryption routine that first gains control of the computer, then decrypts the virus body. However, a polymorphic virus adds to these two components a third — a mutation engine that generates randomized decryption routines that change each time a virus infects a new program. In a polymorphic virus, the mutation engine and virus body are both encrypted. When a user runs a program infected with a polymorphic virus, the decryption routine first gains control of the computer, then decrypts both the virus body and the mutation engine. Next, the decryption routine transfers control of the computer to the virus, which locates a new program to infect. At this point, the virus makes a copy of both itself and the mutation engine in random access memory (RAM). The virus then invokes the mutation engine, which randomly generates a new decryption routine that is capable of decrypting the virus, yet bears little or no resemblance to any prior decryption routine. Next, the virus encrypts this new copy of the virus body and mutation engine. Finally, the virus appends this new decryp-

tion routine, along with the newly encrypted virus and mutation engine, onto a new program. See figures below;

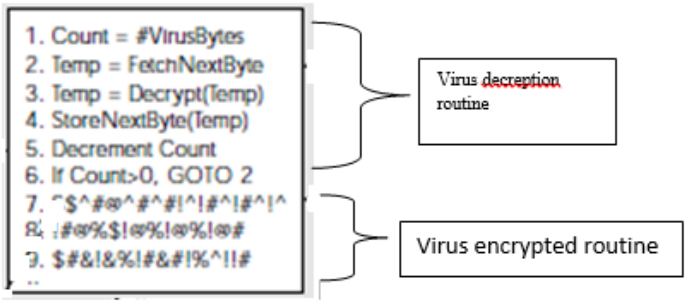

Figure 2 step 1 sample of encrypted virus code before execution

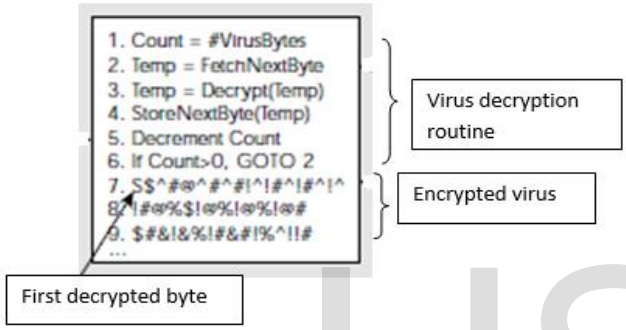

Fig3 Step2 decryption of encrypted virus starts with first stage

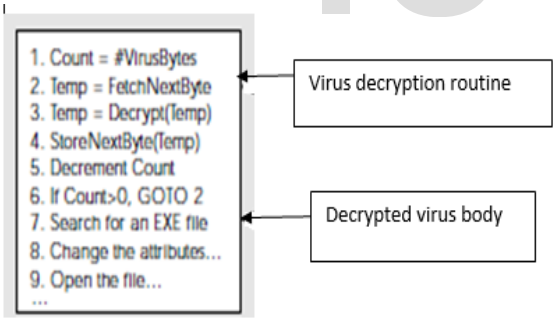

Fig 4 last step fully decrypted virus code.

As a result, not only is the virus body encrypted, but the virus decryption routine varies from infection
to infection. To encrypt the copy of the virus body, an encrypted virus uses an encryption key that the virus is programmed to change from infection to infection. As this key changes, the scrambling of the virus body changes, making the virus appear different from one infection to another infection. This makes it extremely difficult for anti-virus software to search for a virus signature extracted from a consistent virus body. However, the decryption routines remain constant from generation to generation a weakness that anti-virus software quickly evolved to exploit. Instead of scanning just for virus signatures, virus scanners were modified to also search for the sequence of bytes that identified a specific decryption routine. It also has a distractive effect, its target is to encrypt the hard disk and make it unreadable, example is Satan Bug.Natas which is specialized in attacking the antivirus software.

3 METHODS OF VIRUS DETECTION

There are many ways of detecting virus infection , they include the following;

3.1 Static Detection Methods

With static analysis, a virus is detected by examining the files or records for the occurrences of virus patterns without actually running any code. Static Methods include the following methods:

3.1.1 String Scanning Method: This Method Searches For Sequence of bytes (strings) that are
typical of a specific virus but not likely to be found in other programs.

3.1.2 Wildcards Method: This allows to skip bytes or byte ranges. For example "?" character are skipped and the wildcard % means that the scanner will try to match the next byte.

3.1.3. Mismatches Method: allows any given number of bytes in a string to be of arbitrary value, regardless of their position.

3.1.4 Generic Detection Method: This technique uses one common string to detect several or all known variants of a family of viruses.

3.1.5 Bookmarks Method: this method calculates the distance between the start of the virus body and the detection string.

3.1.6 Smart Scanning: Smart scanning could skip junk instructions, such as NOPs, in the host file and also does not store them in the virus signature. To enhance the likelihood of detecting related variants of viruses, an area of the virus body will be selected which had no references to data or other subroutines.

3.1.7 Skeleton Detection: The scanner parses the statements of the virus line-by-line and drops all nonessential statements. What will be left is the skeleton of the body that has only essential macro code common in macro virus.

3.1.8 Heuristics Analysis: Heuristic analysis is an expert based analysis that determines the susceptibility of a system towards particular threat/risk using various decision rules or weighing methods. Multi Criteria analysis (MCA) is one of the means of doing this.

3.1.9 Virus specific detection: There are cases when the standard algorithm of the virus scanner cannot deal with a virus. In cases like this, a new detection code must be introduced to implement a virus-specific detection algorithm. This method includes Filtering, Decrypt or Detection and X-Ray scanning.

3.2 Dynamic Detection Methods

Dynamic detection method decides whether or not code is infected by running the code and observing its behavior. The program monitors known methods of virus activity including attempts to infect and evade detection. This may also include attempts to write to boot sectors, modify interrupt vectors, write to system files, etc. For example, most virus activity eventually needs to call some system functionality, like input/output operations - only these actions have to be considered. No matter how obfuscated the input/output calls are static, the calls will appear clearly when the code runs. Software monitors work best when the normal usage 33 Computer Virus Strategies and Detection Methods characteristics of the system are vastly different from the activity profile of an infected system. A virus might exhibit a dynamic signature like [6] Opening an executable, with both read and write permission.

- Reading the portion of the file header containing the executable start address.
- Writing the same portion of the file header.
- Seeking to the end of the file and
- Appending to the file.

A behavior blocker is antivirus software which monitors a running program's behavior in real time, watching for suspicious activity. If such activity is seen, the behavior blocker can prevent the suspect operations from succeeding, can terminate the program, or can ask the user for the appropriate action to perform. Behavior blocking allowed code to run on the real machine. In contrast, antivirus techniques using emulation let the code being analyzed run in an emulated environment. The hope is that, under emulation, a virus will reveal itself, because any virus found would not be running on the real computer, and it will be harmless.

.

4 WORMS are self-replicating viruses that are loaded into computer memory rather than altering files on the machine. A worm's main goal in life is to spread to as many other machines as possible. It can also be referred to as a program that replicates itself across the network (usually riding on email messages or attached documents (e.g., macro viruses). Worms are spread primarily over the Internet. It is capable of doing this without any input from the user. Worms are distinct from viruses in that they do not require a host program to run, but like viruses, they almost always cause damage to the infected computer.

4.1 Type of Worms

We have different types of worms, they include the following:

4.1.1 Email Worm

An email worms uses a PC's email client to spread itself. It will either send a link within the email that, when clicked, will infect the computer, or it will send an attachment that, when opened, will start the infection. Once the worm is installed, it will search the host computer for any email addresses contained on it. It will then start the process again, sending the worm without any input from the user.

4.1.2 Internet Worms

Internet worms are completely autonomous programs. They use an infected machine to scan the Internet for other vulnerable machines. When a vulnerable machine is located, the worm will infect it and begin the process again. Internet worms are often created to exploit recently discovered security issues on machines that haven't installed the latest operating-system and security updates.

4.1.3 File-sharing Networks Worms

File-sharing worms take advantage of the fact that file-sharers do not know exactly what they are downloading. The worm will copy itself into a shared folder with an unassuming name. When another user on the network downloads files from the shared folder, they will unwittingly download the worm, which then copies itself and repeats the process. In 2004, a worm called "Phatbot" infected millions of computers in this way, and had the ability to steal personal information, including credit card details, and send spam on an unprecedented scale.

4.1.4 Instant Message and Chat Room Worms

These work in a similar way to email worms. The infected worm will use the contact list of the user's chat-room profile or instant-message program to send links to infected websites. These are not as effective as email worms as the recipient needs to accept the message and click the link. They tend to affect only the users of the particular program.

5. CONTROL AND PREVENTION OF VIRUSES AND WORMS

Worms spread by exploiting vulnerabilities in operating systems. Vendors with security problems supply regular security updates and if these are installed to a machine then the majority of worms are unable to spread to it. If vulnerability is disclosed before the security patch is released by the vendor, a zero-day attack is possible. Users need to be aware of opening unexpected email, and should not run attached files or programs, or visit web sites that are linked to such emails. How-

ever, as with the I LOVEYOU worm, and with the increased growth and efficiency of phishing attacks, it remains possible to trick the end-user into running a malicious code. Anti-virus and anti-spyware software are helpful, but must be kept up-to-date with new pattern files at least every few days. The use of a firewall is also recommended. Fortunately, protecting your computer from unwanted intrusions is simpler than you may think. With a few simple steps and adjustments to how you think about surfing and downloading from the Internet, you can increase your computing safety dramatically.

5.1 Anti-Virus Software And Other Preventive Measures

Many users install anti-virus software that can detect and eliminate known viruses after the computer downloads or runs the executable. There are two common methods that an anti-virus software application uses to detect viruses. The first, and by far the most common method of virus detection is using a list of virus signature definitions. This works by examining the content of the computer's memory (its RAM, and boot sectors) and the files stored on fixed or removable drives (hard drives, floppy drives), and comparing those files against a database of known virus "signatures". The disadvantage of this detection method is that users are only protected from viruses that pre-date their last virus definition update. The second method is to use a heuristic algorithm to find viruses based on common behaviors. This method has the ability to detect novel viruses that anti-virus security firms have yet to create a signature for. Some anti-virus programs are able to scan opened files in addition to sent and received email messages "on the fly" in a similar manner. This practice is known as "on-access scanning". Anti-virus software does not change the underlying capability of host software to transmit viruses. Users must update their software regularly to patch security holes. Anti-virus software also needs to be regularly updated in order to recognize the latest threats. One may also minimize the damage done by viruses by making regular backups of data (and the operating systems) on different media, that are either kept unconnected to the system (most of the time), read-only or not accessible for other reasons, such as using different file systems. This way, if data is lost through a virus, one can start again using the backup (which should preferably be recent).

If a backup session on optical media like CD and DVD is closed, it becomes read-only and can no longer be affected by a virus (so long as a virus or infected file was not copied onto the CD/DVD). Likewise, an operating system on a bootable CD can be used to start the computer if the installed operating systems become unusable. Backups on removable media must be carefully inspected before restoration. The Gammima virus, for example, propagates via removable flash drives.

5.2 Be A Suspicious User.

Do not open attachments directly from your e-mail. Instead, save them to a location on the hard drive where your virus scanner will have the opportunity to examine it before you open it.Be cautious when clicking on links in emails. To preview the true link path, however your mouse cursor above the link and looking at the bottom of your email window. If the URL appears to be garbage text or includes a long string of numbers before the actual link, it's probably not legitimate .Never “unsubscribe” to junk by clicking a "remove me" link in an email. [7] Remove me" options on spam are often fake. That is, if you respond to request removal, you very well may be subjecting yourself to more spam, because by responding, the sender knows that your e-mail account is active. A 2002 study performed by the FTC demonstrated that in 63% of the cases where a spam offered a "remove me" option, responding either did nothing or resulted in more e-mail.

5.3 Be A Cautious Internet Surfer.

Do not click “Yes” or “No” or “Cancel” on pop-up windows. Clicking can cause a drive-by download, where software is dropped onto your computer, without your knowledge, no matter which of the three responses you choose. Instead, find the page on the taskbar, right-click on it and select Close. Use the built-in popup blockers that come with most current Internet browsers.

5. 4 Recognizing The Signs

How can you tell if your PC has been compromised by an intrusion, virus, worm, or excessive amount of adware and spyware? The most common signs are: check your browser home page, has it changed and reverts to the new one after reboot, even if you manually changed it. Mistyping a URL redirects you to an odd web site.

Check if you have new toolbars, favorites and/or icons on your desktop without any action by you.Some sites, such as Microsoft Updates or reputable antivirus and spyware removal sites no longer connect/function. Clicking their links leads you to what appear to be junk sites.

Check the speed of your PC, it will slow to a crawl and takes forever to boot.

If your intrusion includes viruses, your antivirus software may also be disabled or unable to update.

6. CONCLUSIONS

The number of computer viruses found in the world is increasing each year. Every time software and antivirus software de-

velopers invent new technology to prevent virus infection, computer virus writers thrilled the world with their ability to go around the new technology and develop the right virus for each age. [8] Macro viruses were their ideal proof of their intention to accept the challenge and cope with the new technology developments. Script viruses were another prove, they have the ability to encrypt each time its reproduced to have a different signature in order to deceive the antivirus and remain undetected The antivirus developer's reaction to this challenge is to develop their programs to detect the pattern in the decryption of the virus, virus writers reaction was creating polymorphic viruses So the mal ware will go on between software and antivirus software developers and virus writers Computer virus writers are not a homogenous group, their motivations could be the need to express their dissatisfaction with their social level, draw attention, become famous and well known, to achieve their revenge, or to prove their technical ability. It seems that the virus writers desire to accomplish their goal conceals their vision from viewing the ethical and legal issues. Another reason could be their dissatisfaction with their society, since the ethics and legal codes belongs to it, and they want revenge for everything in their society including the ethics and legal codes. The legal penalties are not deterring virus writers, but seems to encourage the writers to accept the challenge of writing and releasing a virus to cause the maximum destruction and get away with it or cause serious damage and become famous. By comparing the increasing number of home users with the increasing number of computer viruses each year, we can easily realize the growing threat of computer viruses towards home users. The increasing awareness of computer viruses and basic IT security principles will help home users to eliminate the threat of computer viruses

References

1. http://files-recovery.blogspot.com/2010/06/20-common-types-of-computer-viruses-and.html
2. http://compnetworking.about.com/cs/worldwideweb/g/bldef_worm.htm
3. http://www.emis.de/journals/IJOPCM/files/IJOPCM%28vol.1.2.3.S.08%29.pdf
4. M.E Ezema , H.C. Inyiama.,(2013) Contemporary Malicious Code Detection-TechniquesInternational Journal of Engineering Research and Technology (IJERT)ISSN: 2278- 0181, Vol 2 ,Issue 10, page 2894-2904 http://www.ijert.org
5. http://www.allaboutcookies.org/security/
6. http://www.pctools.com/security-news/what-is-a-macro-virus/
7. https://epic.org/privacy/junk_mail/spam/
8. http://www.ijens.org/100403-5959%20IJECS-IJENS.pdf