Computer Virus: The Treats and Remedies

By

AKPAN, E. Ebenezer, *Ph.D, FCICN, AP, PPGDCA, PHDCDPM*

&

ENIEFIOK, Victor Attah
Corporate Institute of Research and Computer Science
140 Ikot Ekpene Road
Uyo, Akwa Ibom State

ABSTRACT

Computer virus replicates itself by modifying other computer programs and inserting its own code. "Malware" encompasses computer viruses along with many other forms of malicious software, Viruses often perform some type of harmful activity on infected host computers, modify other software without user consent. The first academic work on the theory of self-replicating computer programs was done by John von Neumann. One manner of classifying viruses is to analyze whether they reside in binary executables, one may reduce the damage done by viruses by making regular backups and reinstalling the Operating system. One of the recommendations was that if a computer is being attacked by a virus, the user should reinstall the operating system in order to block the spread of the virus to other folders in the computer.

Key Words: Computer Virus, Malware, Anti-Virus.

Introduction

A computer virus is a type of computer program that, when executed, replicates itself by modifying other computer programs and inserting its own code. When this replication succeeds, the affected areas is then said to be "infected" with a computer virus (Aycock John, 2006).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 ransom ware), desire to send a political message, personal amusement, to demonstrate that a vulnerability exists in software, for sabotage and denial of service, or simply because they wish to explore cyber security issues, artificial life and evolutionary algorithms (Filiol, Eric, 2005).

The term "virus" is also misused by extension to refer to other types of malware. "Malware" encompasses computer viruses along with many other forms of malicious software, such as computer "worms", ransomware, spyware, adware, trojan horses, keyloggers, rootkits, bootkits, malicious Browser Helper Object (BHOs), and other malicious software. The majority of active malware threats are actually Trojan horse programs or computer worms rather than computer viruses.

Statement of the Problem

Computer viruses currently cause billions of dollars' worth of economic damage each year, due to causing system failure, wasting computer resources, corrupting data, increasing maintenance costs, stealing personal information etc. In response, free, open-source antivirus tools have been developed, and an industry of antivirus software has cropped up, selling or freely distributing virus protection to users of various operating systems. As of 2005, even though no currently existing antivirus software was able to uncover all computer viruses (especially new ones), computer security researchers are actively searching for new ways to enable antivirus solutions to more effectively detect emerging viruses, before they have already become widely distributed.

Objective of the Study

The main objective of the study is to examine the threat of computer virus and the remedy. The following objectives were drawn:

1. To find out the threat of computer virus

2. To find out the solution to computer virus.

3. To examine the origin of computer virus

Literature Review

Historical Development of Computer Virus

Early Academic Work on Self-replicating Programs

The first academic work on the theory of self-replicating computer programs was done in 1949 by John von Neumann who gave lectures at the University of Illinois about the "Theory and Organization of Complicated Automata". The work of von Neumann was later published as the "Theory of self-reproducing automata". In his essay von Neumann described how a computer program could be designed to reproduce itself. Von Neumann's design for a self-reproducing computer program is considered the world's first computer virus, and he is considered to be the theoretical "father" of computer virology. In his work Kraus postulated that computer programs can act in a way similar to biological viruses.

Operations and Function of Computer Virus

Parts: A viable computer virus must contain a search routine, which locates new files or new disks which are worthwhile targets for infection. Secondly, every computer virus must contain a routine to copy itself into the program that the search routine locates. (Ludwig, Mark 2000) some virus parts are:

Trigger: The trigger, which is also known as a logic bomb, is the compiled version that could be activated any time within an executable file especially when the virus determines the event or condition for the malicious "payload" to be activated or delivered such as a particular date, time, and a particular presence of another program, capacity of the disk exceeding some limit, or a double-click that opens a particular file. **(**Gregory, Peter 2004)

Payload: The "payload" is the actual body or data that performs the actual malicious purpose of the virus. Payload activity might be noticeable (e.g., because it causes the system to slow down or "freeze"), as most of the time the "payload" itself is the harmful activity, or sometimes non-destructive but distributive, which is called Virus hoax. (Szor, Peter 2005)

Phases: Virus phases is the life cycle of the computer virus, described by using an analogy to biology. This life cycle can be divided into four phases: dormant phase (The virus program is idle during this stage), propagation phase (The virus starts propagating, that is multiplying and replicating itself), Triggering phase (A dormant virus moves into this phase when it is activated, and will now perform the function for which it was intended) and execution phase (This is the actual work of the virus, where the "payload" will be released). (Stallings, William 2012)

Infection Targets and Replication Techniques

Computer viruses infect a variety of different subsystems on their host computers and software. One manner of classifying viruses is to analyze whether they reside in binary executables data files such as (Microsoft Word documents or PDF files), or in the boot sector of the host's hard drive (or some combination of all of these).

Resident VS. Non-Resident Viruses

A *memory-resident virus* (or simply "resident virus") installs itself as part of the operating system when executed, after which it remains in RAM from the time the computer is booted up to when it is shut down. Resident viruses overwrite interrupt handling code or other functions, and when the operating system attempts to access the target file or disk sector, the virus code intercepts the request and redirects the control flow to the replication module, infecting the target. In contrast, a *non-memory-resident virus* (or "non-resident virus"), when executed they scans the disk for targets, infects them, and then exits (i.e. it does not remain in memory after it is done executing). (Salomon, David 2006)

Macro viruses: Many common applications, such as Microsoft Outlook and Microsoft Word, allow macro programs to be embedded in documents or emails, so that the programs may function automatically when the document is opened. A *macro virus* (or "document virus") is a virus that is written in a macro language, and embedded into these documents so that when users open the file, the virus code is executed, and can infect the user's computer.

Boot sector viruses: *Boot sector viruses* specifically target the boot sector and/or the Master Boot Record(MBR) of the host's hard disk drive, solid-state drive, or removable storage media (flash drives, floppy disks, etc.).

Email virus: Email virus are viruses that intentionally, rather than accidentally, uses the email system to spread. While virus infected files may be accidentally sent as email attachments, email viruses are aware of email system functions. They generally target a specific type of email system (Microsoft's Outlook is the most commonly used), harvest email addresses from various sources, and may append copies of themselves to all email sent, or may generate email messages containing copies of themselves as attachments. (Dave Jones (December 2001)

Read request intercepts: While some kinds of antivirus software employ various techniques to counter stealth mechanisms, once the infection occurs any recourse to "clean" the system is unreliable. In Microsoft Windows operating systems, the NTFS file system is proprietary. This leaves antivirus software little alternative but to send a "read" request to Windows files that handle such requests. Some viruses trick antivirus software by intercepting its requests to the operating system. A virus can hide by intercepting the request to read the infected file, handling the request itself, and returning an uninfected version of the file to the antivirus software. The interception can occur by code injection of the actual operating system files that would handle the read request. Thus, an antivirus software attempting to detect the virus will either not be given permission to read the infected file, or, the "read" request will be served with the uninfected version of the same file. (Szor, Peter 2005).

Self-modification: Most modern antivirus programs try to find virus-patterns inside ordinary programs by scanning them for so-called *virus signatures*. **(**Jacobs, Stuart 2015-12-01) Unfortunately, the term is misleading, in that viruses do not possess unique signatures in the way that human beings do. Such a virus "signature" is merely a sequence of bytes that an antivirus program looks for because it is known to be part of the virus. A better term would be "search strings". Different antivirus programs will employ different search strings, and indeed different search methods, when identifying viruses. If a virus scanner finds such a pattern in a file, it will perform other checks to make sure that it has found the virus, and not merely a coincidental sequence in an innocent file, before it notifies the user that the file is infected.

Encrypted viruses: One method of evading signature detection is to use simple encryption to encipher (encode) the body of the virus, leaving only the encryption module and a static cryptographic key in clear text which does not change from one infection to the next.**(**Bishop, Matt 2003)In this case, the virus consists of a small decrypting module and an encrypted copy of the virus code. If the virus is encrypted with a different key for each infected file, the only part of the virus that remains constant is the decrypting module, which would be appended to the end.

Polymorphic code: Polymorphic code was the first technique that posed a serious threat to virus scanners. Just like regular encrypted viruses, a polymorphic virus infects files with an encrypted copy of itself, which is decoded by a decryption module. In the case of polymorphic viruses, however, this decryption module is also modified on each infection. A well-written polymorphic virus therefore has no parts which remain identical between infections, making it very difficult to detect directly using "signatures" Antivirus software can detect it by decrypting the viruses using an emulator, or by statistical pattern analysis of the encrypted virus body. To enable polymorphic code, the virus has to have a polymorphic engine (also called "mutating engine" or "mutation engine") somewhere in its encrypted body.

Metamorphic code: To avoid being detected by emulation, some viruses rewrite themselves completely each time they are to infect new executables. Viruses that utilize this technique are said to be in metamorphic code. To enable metamorphism, a "metamorphic engine" is needed. A metamorphic virus is usually very large and complex.

Software bugs: As software is often designed with security features to prevent unauthorized use of system resources, many viruses must exploit and manipulate security bugs, which are security defects in a system or application software, to spread themselves and infect other computers. Software development strategies that produce large numbers of "bugs" will generally also produce potential exploitable "holes" or "entrances" for the virus.

Vulnerability of Different Operating Systems

The vast majority of viruses target systems running Microsoft Windows. This is due to Microsoft's large market share of desktop computer users. The diversity of software systems on a network limits the destructive potential of viruses and malware. Open-source operating systems such as Linux allow users to choose from a variety of desktop environments, packaging tools, etc., which means that malicious code targeting any of these systems will only affect a subset of all users. Many Windows users are running the same set of applications, enabling viruses to rapidly spread among Microsoft Windows systems by targeting the same exploits on large numbers of hosts.

While Linux and Unix in general have always natively prevented normal users from making changes to the operating system environment without permission, Windows users are generally not prevented from making these changes, which implies that viruses can easily gain control of the entire system on Windows hosts. (Boldt, Axel 19 January 2000)

Countermeasures

Antivirus Software

Many users install antivirus software that can detect and eliminate known viruses when the computer attempts to download or run the executable file (which may be distributed as an email attachment, or on USB flash drives, for example). Some antivirus software blocks known malicious websites that attempt to install malware. Antivirus software does not change the underlying capability of hosts to transmit viruses. Users must update their software regularly to patch security vulnerabilities ("holes"). Antivirus software also needs to be regularly updated in order to recognize the latest threats. This is because malicious hackers and other individuals are always creating new viruses. The German AVTEST Institute publishes evaluations of antivirus software for Windows and Android

Recovery Strategies and Methods

One may reduce 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, as in a hard drive), read-only or not accessible for other reasons, such as using different file systems.

Virus removal

Many websites run by antivirus software companies provide free online virus scanning, with limited "cleaning" facilities (after all, the purpose of the websites is to sell antivirus products and services). Some websites—like Google subsidiary VirusTotal.com—allow users to upload one or more suspicious files to be scanned and checked by one or more antivirus programs in one operation. Additionally, several capable antivirus software programs are available for free download from the Internet (usually restricted to non-commercial use). Microsoft offers an optional free antivirus utility called Microsoft Security Essentials, a Windows Malicious Software Removal Tool that is updated as part of the regular Windows update regime, and an older optional anti-malware (malware removal) tool Windows Defender that has been upgraded to an antivirus product in Windows 8. Some viruses disable System Restore and other important Windows tools such as Task Manager and CMD (Virus removal 2015-01-31).

Operating system reinstallation

Microsoft's System File Checker (improved in Windows 7) can be used to check, and repair, corrupted system files. Restoring an earlier "clean" (virus-free) copy of the entire partition from a cloned disk, a disk image, or a backup copy is one solution—restoring an earlier backup disk "image" is relatively simple to do, usually removes any malware, and may be faster than "disinfecting" the computer—or reinstalling and reconfiguring the operating system and programs from scratch, as described below, then restoring user preferences. Reinstalling the operating system is another approach to virus removal. It may be possible to recover copies of essential user data by booting from a live CD, or connecting the hard drive to another computer and booting from the second computer's operating system, taking great care not to infect that computer by executing any infected programs on the original drive. The original hard drive can then be reformatted and the OS and all programs installed from original media. Once the system has been restored, precautions must be taken to avoid reinfection from any restored executable files. (us-cert.gov(PDF) 2016-04-19)

Conclusion

In conclusion, computer virus has posed a great threat to computer files by modifying other computer programs and inserting its own code. Computer viruses currently cause billions of dollars' worth of economic damage each year, due to causing system failure, wasting computer resources, corrupting data, increasing maintenance costs, stealing personal information etc. In response, free, open-source antivirus tools have been developed, and an industry of antivirus software has cropped up, selling or freely distributing virus protection to users of various operating systems. So users are expected to update their software regularly to patch and recognize the latest threats security vulnerabilities ("holes").

Recommendation

Due to the threat of computer virus, the following recommendations are deemed necessary.

1. Computer users should install an antivirus software in their computer to help prevent them against the treat of computer virus.

2. If a computer is being attacked by a virus, the user should reinstall the operating system in order to block the spread of the virus to other folders in the computer.

3. Computer files should always be backed up to another file or disk so that if the one in the computer is being affected by a virus, the backup can be used.

REFERENCES

Aycock, John (2006). *Computer Viruses and Malware*. Springer. p. 14.

Filiol, Eric (2005). *Computer viruses:* from theory to applications. Springer. p. 8.

Kaspersky, Eugene (November 21, 2005). *"The contemporary antivirus industry and its problems"*. Secure Light. Archived from the original on

Ludwig, Mark (2000). *The giant black book of computer viruses*. Show Low, Ariz: American Eagle. p. 15.

Gregory, Peter (2004). *Computer viruses for dummies* (in Danish). Hoboken, NJ: Wiley Pub. p. 210.

Szor, Peter (2005). *The art of computer virus research and defense*. Upper Saddle River, NJ: Addison-Wesley. p. 43.

Stallings, William (2012). *Computer security: principles and practice*. Boston: Pearson. p. 183.

Salomon, David (2006). *Foundations of Computer Security*. Springer. pp. 47–48.

Dave Jones. 2001 (2001). "Building an e-mail virus detection system for your network. Linux J. 2001, 92, 2-".

Szor, Peter (2005). *The Art of Computer Virus Research and Defense*. Boston: Addison-Wesley. p. 285.

Jacobs, Stuart (2015-12-01). *Engineering Information Security: The Application of Systems Engineering Concepts to Achieve Information Assurance*. John Wiley & Sons.

Bishop, Matt (2003). *Computer Security: Art and Science*. Addison-Wesley Professional. p. 620.