Threats to Digitization: Computer Virus

Bhaskar Mukherjee

Abstract

Discusses historical background of Internet and pointed out how threats to digitization has increased with the development of Internet. The paper mentioned common symptoms of virus infection and suggests some measures towards protecting computers from virus as recommended by Microsoft and Symantec Corporation. Also lists some authorized anti-virus software available on Internet.

Keywords: Computer Virus, Computer Network, Internet, Anti-Virus

1. Introduction

The tremendous development of computer science and communication technology gives some unique invention to us. But with these development life becomes more complex. In present era, Internet evolves as immense tool ever devised in information retrieval. In these vast interconnected global network, Internet brings a free flow of data and information to ten millions of people throughout the world. Internet is being used to access or to exchange information via email, newsgroup, searching. At the same time, Internet access has opened a Pandora's box of issues, each of which poses serious threats to our productivity and profitability. An unfortunate side effect of Internet maturity and progress is that adversaries can enjoy equal success. Email and other Internet traffic such as FTP downloads can serve as a carrier for damaging viruses and other malicious code capable of interfacing entire networks. Electronic mail, the principal mean of communication is the most primary carrier of viruses and Trojans. It has been estimated that 80% of all virus infection are now due to macro viruses, hidden inside word processing and spreadsheet files that are attached to emails. The advent of software, Active-X, Java applets that allow web pages to be transferred via email provides a powerful new transmission route for malicious code. These malicious codes have shown that today's adversaries are employing new combinations of offences against Information technology infrastructure. 'One threat-One cure' has become outdated. Present threats of these malicious codes graphically point out that mere single point of solution will no longer be adequate to address them. It is also necessary to protect all parts of network and respond on the gateway, server and client level. The birth of Nimda, CodeRed, W32/Klez, Blaster, W32/Sassar reminds us the unfortunate side effect of advanced technology. Subsequently flood of these viruses and spams impact our productivity as well as network performance with tremendous loss of money, materials and time too. The restoration of program/ data to its original or to update/ maintains the infrastructure to its operational condition including an administrative overhead.

2. Internet – A Short History

The success story of Internet starts a long back when Cook and Whealstone has developed telegraph in 1836. Afterwards the invention of Trans-satellite cable during 1858-66; telephone by Alexander

Graham Bell in 1876; Sputnik by USSR in 1957 and concept of packet switching during 1962-68 adds a revolutionary jump in communication technology. The story of networking starts from August, 1962 when J.C.R. Licklider of Massachusetts Institute of Technology (MIT) envisioning the idea of "Garlic Network" of globally interconnected set of computers through which everyone could quickly access data and pages from any site. After nuclear war, the RAND Corporation, American's cold war think-tank faced a strange strategic problem to communicate US authorities. This post nuclear America was needed a command-and-control network, linked from city to city, state to state and so on. Although Paul Baran proposal of 1964 puts a new venture regarding this problem but first successful network named ARPANET was been successfully installed by United States Defense Advanced Research Project Agency (ARPA) during 1969 to communicate four nodes. Subsequently in Europe, National Physical Laboratory of Great Britain developed Test Network on this principle during 1968. During 1971, there were fifteen nodes in ARPANET; and by 1972 it increased to 37 nodes. The ARPA's original standard for communication was known as NCP "Network Control Protocol" which with passages of time and advancement of techniques, later on changed to high-level, more sophisticated standard known as TCP/IP. TCP or Transmission Control Protocol converts message into stream of packets at the source, then resembles them back into message at the destination. IP or Internet Protocol handles the addressing, seeing to it that packets are routed across multiples nodes and even across multiple network with multiple standard not only ARPA's pioneering NCP standard, but also others like Ethernet, FDDI and X.25.

Internet was based on the idea that there would be multiple independent networks of rather arbitrary design, beginning with the ARPANET as the pioneering packet switching network, but soon to include packet satellite networks, ground-based packet radio networks and other networks. The Internet as we now knows it embodies a key underlying technical idea, namely that of opens architecture networking. In this approach, the choice of any individual network technology was not dictated by particular network architecture but rather could be selected freely by a provider and made to inter-work with the other networks through a meta-level "Internetworking Architecture".

Widespread development of LANS, PCs and workstations in the 1980s allowed the nascent Internet to flourish. Ethernet technology, developed by Bob Metcalfe at Xerox PARC in 1973, is now probably the dominant network technology in the Internet and PCs and workstations the dominant computers. This change from having a few networks with a modest number of time-shared hosts (the original ARPANET model) to having many networks has resulted in a number of new concepts and changes to the underlying technology. First, it resulted in the definition of three network classes (A, B, and C) to accommodate the range of networks. Class A represented large national scale networks (small number of networks with large numbers of hosts); Class B represented regional scale networks; and Class C represented local area networks (large number of networks with relatively few hosts).

A major shift occurred as a result of the increase in scale of the Internet and its associated management issues. To make it easy for people to use the network, hosts were assigned names, so that it was not necessary to remember the numeric addresses. Originally, there were a fairly limited number of hosts, so it was feasible to maintain a single table of all the hosts and their associated names and addresses. The shift to having a large number of independently managed networks (e.g., LANs) meant that having a single table of hosts was no longer feasible, and Paul Mockapetris of USC/ISI invented the Domain Name System (DNS). The DNS permitted a scalable distributed mechanism for resolving hierarchical host names into an Internet address.

The increase in the size of the Internet also challenged the capabilities of the routers. Originally, there was a single distributed algorithm for routing that was implemented uniformly by all the routers in the Internet. As the number of networks in the Internet exploded, this initial design could not expand as necessary, so it was replaced by a hierarchical model of routing, with an Interior Gateway Protocol (IGP) used inside each region of the Internet, and an Exterior Gateway Protocol (EGP) used to tie the regions together. This design permitted different regions to use a different IGP, so that different requirements for cost, rapid reconfiguration, robustness and scale could be accommodated. Not only the routing algorithm, but also the size of the addressing tables, stressed the capacity of the routers. New approaches for address aggregation, in particular classless inter-domain routing (CIDR), have recently been introduced to control the size of router tables.

One should not conclude that the Internet has now finished changing. The Internet, although a network in name and geography is a creature of the computer, not the traditional network of the telephone or television industry. It will, indeed it must, continue to change and evolve at the speed of the computer industry if it is to remain relevant. It is now changing to provide such new services as real time transport, in order to support, for example, audio and video streams. The availability of pervasive networking (i.e., the Internet) along with powerful affordable computing and communications in portable form (i.e., laptop computers, two-way pagers, PDAs, cellular phones), is making possible a new paradigm of nomadic computing and communications.

3. Virus- The Treats of IT

As computer progressed, the brain of intellectuals also stimulate to develop some unwanted/ destructive codes/ logic, which 'broke-the-bound' of useful program and would either perform operations on the data or programs belonging to different procedure, or actually transferred control to random areas and tried to execute data as program instructions.

A virus is code written with the express intention that the virus code replicates itself. A virus tries to spread itself from computer to computer by attaching itself to a host program. It may damage hardware, software, or data. A worm is a subclass of virus. A worm generally spreads without user action and distributes complete copies (possibly modified) of itself across networks. A worm can exhaust memory or network bandwidth, causing a computer to stop responding. A virus that appears to be a useful program, but that actually does damage, is a "trojan horse."

The term is some time also used for viral programs which spread by some method viz attachment, association with original code/ program and spread from one computer to another. One of the factors involved in the success of viral programs is a study of the mindset of the user: a study of the psychology or sociology of the computer community. Since the spread of viral programs generally require some action, albeit unknowing, on the part of the operator, it is instructive to look at the security breaking aspects of other historical programs.

Although the birth of virus is not as long as internet but since last decade its replication and number increased in such a manner that in present day its total number is anybodies guess. In present day more than 200 viruses are found in each month. Let us see its history.

The first virus Brain was noted in 1986 which was written by Pakistan. The brain was a boot-sector virus, which means it only infected the boot records of 360K floppy disks, but not hard drives. It would occupy unused space on the disk so that it could not be used. It was also the first "stealth" virus, meaning it tried to hide itself from detection. If a computer user tried to view the infected space on the disk, Brain would display the original, uninfected boot sector. First file infecting memory resident Lehigh virus was noted in 1987 as executable file virus that attacks COMMAND.COM file. In 1988 first encrypted virus Cascade was found in Germany. Dark Avenger was introduced in virus history in 1989, which was designed to damage a system slowly, so it would go unnoticed at first and damage file would be backed up. During 1994-1999 number of notorious viruses has also developed such as Kaos4, Boza, Laroux, Melissa etc. But in year 2000 "I Love You Virus" wreaks havoc around the world. It is transmitted by email and when opened, it automatically sent to everyone in the user's address book. In 18 September, 2001 the birth of Nimda and subsequently CodeRed worms creates a panic to computer world. The differential feature of Nimda was that it requires no human interaction to spread, instead using known software vulnerabilities and multiple vector infection. It was estimated that during 2:30 PM on Sept 20 and 2:30 PM, Sept' 21 Nimda infected over 2.2 million servers and PCs which cause a total loss of $10.7 billion. Nimda propagate through network looking for unpatched Microsoft internet Information Server. It then attempts to use the specific exploit, called Unicode Web Traversal exploit, to gain control of the target server. It also propagate through email by harvesting email addresses from any MAPI compliant email program's mailbox and extract email address from html and htm files. Nimda attacks hard disks of systems that have enabled file sharing over network and create a guest account with administrative privileges.

In present day, PWSteal.Ibank, Trojan. Anits, W32.Klez / Mydoom/ Spybot Bloodhound.Explot.13, Backdoor.Nemog.B, Beagle, W97/ MTX, VBS/SST@MM (Anna Kournikova) Blaster are some of the invention of most notorious virus/worms which all are based on network and spread computer to computer through Internet and LAN. These virus searches for .EXE, .INI, .COM, .DLL, .TXT, .GIF,

.JPG, .JPEG, .MPEG, .MOV, .BAT, .PDF, .PNG, .PS, .ZIP, .VBS, .LOG files and also attack MY DOCUMENTS folder and attempts to send copies of these document to email recipients found in windows address book and address found in cache files.

4. Symptoms of Viruses, Worms and Trojan Horse Viruses

When a virus infects your e-mail or other files, it may have some effects on your computer. Microsoft pointed followings:

- The infected file may make copies of itself. This may use all the free space in your hard disk. A copy of the infected file may be sent to all the addresses in your e-mail address list.
- The virus may reformat your disk drive and delete your files and programs.
- The virus may install hidden programs, such as pirated software. This pirated software may then be distributed and sold from your computer.
- The virus may reduce security. This could allow intruders to remotely access your computer or network.

Following symptoms are frequently visualized with a virus infected computer:

- You received an e-mail message that has a strange attachment. When you open the attachment, dialog boxes appear or a sudden degradation in system performance occurs.
- There is a double extension on an attachment that you recently opened, such as .jpg.vbs or .gif.exe, .doc.scr.
- An antivirus program is disabled for no reason and it cannot be restarted or allow to install antivirus program to the system.
- Strange dialog boxes or message boxes appear onscreen.
- Someone tells you that they have recently received e-mail messages from you containing attached files (especially with .exe, .bat, .scr , and .vbs extensions) that you did not send.
- New icons appear on the desktop that you did not put there, or are not associated with any recently installed programs.
- Strange sounds or music plays from the speakers unexpectedly.
- A program disappears from the computer, but you did not intentionally remove it. A virus infection may also cause the following symptoms, but these symptoms may also be the result of ordinary Windows functions, or problems in Windows that is not caused by a virus.
- Windows will not start at all, even though you have not made any system changes, and you have not installed or removed any programs.
- There is much modem activity. If you have an external modem, you may notice the lights blinking too much when the modem is not being used. You may be unknowingly supplying pirated software.
- Windows will not start because certain critical system files are missing, and then you receive an error message that lists the missing files.

- The computer sometimes starts as expected, but at other times it stops responding before the desktop icons and taskbar appear.
- The computer runs very slowly, and it takes a long time to start.
- You receive out-of-memory error messages even though your computer has much RAM.
- New programs do not install correctly.
- Windows spontaneously restarts unexpectedly.
- Programs that used to run stop responding frequently. If you try to remove and reinstall the software, the issue continues to occur.
- A disk utility such as Scandisk reports multiple serious disk errors.
- A partition disappears.
- Your computer always stops responding when you try to use Microsoft Office products.
- You cannot start Windows Task Manager.
- Antivirus software indicates that a virus is present.

5. Protecting Computer from Virus

Presently maximum viruses are omnipotent in nature, means they does not need to execute but they automatically execute silently in system and spread from one computer to another via LAN, as email attachment, downloadable file or some external link. The common vector of viruses are External network, Guest Client, Executable file, Documents, Emails, Removable media such as CDROM or DVD ROM, Floppy disk, USB Drive, Memory card etc. English proverb "Prevention is better than cure" is quite appropriate way to protect computer from virus, but it is not accepted opinion to most people that, file not to be shared, software not to be down load. So the best possible way is knowledge sharing and awareness. Circulating/hosting news, article describes the destruction or inconveniences caused by malicious code to the web and to aware about virus threats around the people using email, internet. Microsoft has pointed out some common tips to prevent virus, they are

5.1 Use Firewall (for Windows based system)- A firewall is a piece of software or hardware that creates a protective barrier between your computer and potentially damaging content on the Internet. It helps guard your computer against malicious users and many computer viruses and worms.

5.2 Update your computer. - Security updates help shield your computer from vulnerabilities, viruses, worms, and other threats as they are discovered. Steps that you can take include:

a. Install security updates for Windows and Windows components (such as Internet Explorer, Outlook Express, and Windows Media Player).

b. Disable Active Scripting in Outlook and Outlook Express.

c. Install higher version of Service Packs (SP). By default, Outlook Express 6 SP1 blocks access to attachments. Earlier versions of Outlook Express (pre-Outlook Express 6) do not contain attachment-blocking functionality. Use extreme caution when you open unsolicited e-mail messages with attachments.

Vincent Weafer of Symantec corporation recommend following tips –

5.3 Install anti-virus software and keep the virus definitions up to date. Anti-virus software scans files for unusual changes in file size, programs that match the software's database of known viruses, suspicious email attachments, and other warning signs. It's the most important step you can take towards keeping your computer clean of viruses. Subsequently, updating of anti-virus allows updating of current virus definitions which prevent computer with new viruses.

5.4 Don't automatically open attachments and make sure your email program doesn't do so either. This will ensure that you can examine and scan attachments before they run. Refer to your email program's safety options or preferences menu for instructions. Because email message can include file attachment, hackers can send infected files & hope that recipient will open them, as happened with Melissa & Monwells. This methods makes use of social engineers to urge the end user to run the file. Other method exist which allow skilled and possible malevolent crackers to inject code through email and run custom-made applications automatically while the end user recalls the email text. Such problems have been around since the use of HTML in email and have been exploited by notorius worms such as Kak Worms, BubbleBoy virus or Nimda.

5.5 Scan all incoming email attachments. Be sure to run each attachment you plan to open through the anti-virus check. Most anti-virus software can be setup to check files automatically. Do this even if you recognize and trust the sender; malicious code, like trojan horses, can slip into your system by appearing to be from a friendly source. Melissa and Love letter virus were among first viri to illustrated the problem with email attachment and trust. They made use of the trust that exist between friends, colleagues. Upon running such worms usually proceed to send themselves out to email address from the victim's address book, preventing email, webpages caches to the local machines and similar method.

5.6 Get immediate protection. Configure your anti-virus software to boot automatically on start-up and run at all times. In case you forget to boot up your anti-virus software, configuring it to start by itself will ensure you are always protected.

5.7 Update your anti-virus software frequently. An anti-virus program is only as good as the frequency with which it is updated. New viruses, worms, and Trojan horses are born daily, and variations of them can slip by software that is not current. Most anti-virus software is easy to update online with options to do so automatically. Check whether your system has automatically update with new definition or not.

5.8 Avoid downloading files you can't be sure are safe. This includes freeware, screensavers, games, and any other executable program - any files with an ".exe" or ".com" extension such as "coolgame.exe." Unreliable sources such as Internet newsgroups or Web sites that you haven't heard of may be willing providers of viruses for your computer. If you do have to download from the Internet, be sure to scan each program before running it. Save all downloads to one folder, then run virus checks on everything in the folder before using it.

5.9 Don't boot from a floppy disk. Floppies are one of the most common ways viruses are transmitted. If you are using a floppy while working on your computer, remove it when you shut the machine off or the computer will automatically try to boot from the floppy, perhaps launching any viruses on the disk.

5.10 Don't share floppies/ Pen drives. Even a well-meaning friend may unknowingly pass along a virus, trojan horse, or worm. Label your floppies clearly so you know they're yours and don't loan them out. If a friend passes you a floppy/pen drive, suggest an alternative method of file sharing.

5.11 Scan floppies/pen drives before using them. This is always important, but especially if you are using the disk to carry information between one computer and another. You could easily pick up a virus from an insecure network and introduce it into your system. Running a virus scan before launching any of the programs on the disk will prevent infection.

5.12 Use common sense. It's always better to err on the side of safety. If you're unsure about an attachment, delete it. Especially if it's from a source you don't recognize. If there are tempting animations on a site that look highly unprofessional, don't download them. Also beware of strange links or unexpected attachments that come through instant messaging programs. They could hide malicious code.

6. Vaccines / Anti-virus software

To prevent viruses to a computer there are two usual options. In the first way we may protect our machine from viruses by disconnecting it from internet or LAN, not using antyremovable storage disk. By this it will be a perfect data processing machine ... but with no data to process. Computer will be about as much as a micro-oven. The second method is to install antivirus programs and update it frequently. Antivirus program do not perform miracles, nor is it a software tool that you need to be wary of.

Antivirus software of present day enabled with scan engines. This engines scan the information it has intercepted for viruses and if viruses are detected, it disinfect them. The information can be scanned in two ways. One method involves comparing the information received with a virus databases (known as virus signatures) if the information matches any of the virus signature by scanning memory, your files and system sectors, the anti-virus concluded that the file is infected by virus. The other way of finding out if the information being scanned is dangerous, without knowing of it is actually contains a virus or not, is the method known as 'heuristic method'. This method involves analyzing how the information acts and comparing it with a list of dangerous activity patterns. Both the methods have their pros and cons. If only the virus signature system is used, it is important to update it atleast once a day, when you bear in mind that 15 new virus are discovered every day. The drawbacks with heuristic system is that it can warn you about those items too that you known are not virus.

After scanning, some antivirus tools are compatible with disinfector tool. A disinfector like a scanner can very handy tool, but it must be used with care. To remove virus, disinfector, must be current one. But disinfectors some time claims falsely and some time it delete the files when not able to cure. In some cases virus moodily the programs in such a way that removal is not possible, they basically overwrite the part of the programs. In these case antivirus tools fails top cure it and only way left is to restore the infected files from backup, if available otherwise loss. But it is always recommended to install antivirus to protect computers from unwanted threats. Let us keep a look some of available useful antivirus which are widely used in present day as removal tool.

- Norton Anti-virus (latest Ed.) / Symantec Security (http://www.symantec.com)
- McAfee Virus scan (latest Ed.) (http://www.mcafee.com)
- Dr. Solomons Virex (latest Ed.) (www.dealclick.co.uk/product/161582/ Network-Associates-Dr-Solomons-Virex-6-0.php)
- PC-cillin 2007 virus protection (http://www.trendmicro.com/en/products/desktop/pc-cillin/ evaluate/ overview. htm)
- AVG Anti-Virus (http://www.grisoft.com/us/us_index.php)
- F-Prot (http://www.f-prot.com/products/home_use/dos/)
- F-secure (http://www.f-secure.com/weblog/)
- Panda ActiveScan (http://www.pandasoftware.com/products/platinum7/)
- MyDoom Virus remover (http://www.webroot.com/services/mydoomaudit.htm)
- Beagle remover Tool (http://www.webroot.com/services/beagleaudit.htm)
- Active Scan (http://www.pandasoftware.com/activescan/)
- AntiVir PE 6.27.00.03 (http://www.free-av.com/)
- BitDefencer (http://www.bitdefender.com/bd/site/solutions.php?menu_id=8)
- DoctorWeb (http://www.dials.ru/english/dsav_toolkit/drweb32.htm)
- Eicar Anti-virus (http://www.eicar.org/anti_virus_test_file.htm)
- Freem Anti-virus (http://www.freedom.net/products/av/)

7. Conclusion

Threats are expected to appear with increased regularity and growing complexity. The best defense against today's threats consists of adopting best practice and applying them in concert with comprehensive security solutions.

References

1. Microsoft Security & Privacy Home Page. Available at: http://www.microsoft.com/security/default.asp
2. Microsoft Windows Update. Available at: http://v4.windowsupdate.microsoft.com/en/default.asp
3. Symantec Security Response. Available at: http://securityresponse.symantec.com
4. Schneier, Bruce. Applied Cryptography: protocols, Algorithms, and Source Code in C. 2nd Edition, New York: John Wiley & Sons, October 1995.
5. Zwicky, Elizabeth D., Cooper, Simon, and Chapman, D. Brent. Building Internet firewall, 2nd Ed. New York: O'Reilly & Associates, Inc. June 2000.
6. Denning, Peter J. Computer under attack: intruder, worms and viruses. New York: Addison-Wesley, January 1990.
7. Garfinkel, Simson. Database Nation: the death of privacy in 21st century. New York: O'Reilly & Associate Inc., January 2001.
8. Honenet Project: Know your enemy: Revealing the security tool, tactics and motives of Blackhut Community. New York: Addision-Wesley. August 2001.
9. McGraw, Gray and Felten , Edward W. Secret & Lies: digital security in network world. Jon Willey & Sons. January 1999.
10. Pfleeger, Charles. Security in computing. Prentice-Hall, September 1996.
11. Garfinkel, Simson and Spafford, Gene. Web security, privacy and commerce. 2nd ed., New York, O'Reilly Media, Inc., Nov. 2001.

About Author

Dr. Bhaskar Mukherjee, Lecturer, Department of Library and Information Science, Banaras Hindu University, Varanasi (UP)
E-mail: mukherjee.bhaskar@gmail.com