COMPUTER VIRUS AND PENETRATION TECHNIQUE

S. Jeya, A. P./M.C.A.,
K.S.R. College of Engineering,
Thiruchengode, Namakkal,
Tamil Nadu, India,
Email: mayej_s@yahoo.co.in

Dr. K. Ramar,
Professor & HOD/CSE Dept.,
National Engineering College, Kovilpatti,
Tamil Nadu, India.
Email: kramar_nec@rediffmail.com

Abstract
Computer viruses have been around almost as long as computers. Latest technical development such as high speed network, internet & advance personal computers have provided viruses a main threat to the computers. I remember the story of elephant and ant and how the ant brought the mighty elephant down on its knees? Similarly, a computer virus, a few KBs in size, like any piece of code, which when executed on computer, carries out a particular task, can destroy gigabytes of data stored in computer and bring the biggest organization to a halt. A lot of anti-virus software is available in the market and being widely used but these anti-viruses are less effective as they are made only for the existing viruses not for the viruses which developed latter. So this paper mainly concentrates on analyzing the procedures which is being used for preventing virus. Then it covers what strategy should be adopted for anti-virus and how to recover the computer from a virus attack. This paper also describes the identification & classification of computer virus, and current computer virus situation.

Keywords: malware, Trojan horses, arsonists, and Nessus.

1. Introduction

A **computer virus** is a computer program that can copy itself and infect a computer without permission or knowledge of the user. However, the term "virus" is commonly used, albeit erroneously, to refer to many different types of malware programs. The original virus may modify the copies, or the copies may modify themselves, as occurs in a metamorphic virus. A virus can only spread from one computer to another when its host is taken to the uninfected computer, for instance by a user sending it over a network or the Internet, or by carrying it on a removable medium such as a floppy disk, CD, or USB drive. Additionally, viruses can spread to other computers by infecting files on a network file system or a file system that is accessed by another computer. Viruses are sometimes confused with computer worms and Trojan horses. A worm can spread itself to other computers without needing to be transferred as part of a host, and a Trojan horse is a file that appears harmless until executed.

Most personal computers are now connected to the Internet and to local area networks, facilitating the spread of malicious code. Today's viruses may also take advantage of network services such as the World Wide Web, e-mail, and file sharing systems to spread, blurring the line between viruses and worms. Furthermore, some sources use an alternative terminology in which a virus is any form of self-replicating malware.

Some viruses are programmed to damage the computer by damaging programs, deleting files, or reformatting the hard disk. Others are not designed to do any damage, but simply replicate themselves and perhaps make their presence known by presenting text, video, or audio messages. Even these benign viruses can create problems for the computer user. They typically take up computer memory used by legitimate programs. As a result, they often cause erratic behavior and can result in system crashes. In addition, many viruses are bug-ridden, and these bugs may lead to system crashes and data loss.

Computer viruses are small software programs that are designed to spread from one computer to another and to interfere with computer operation. 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 [9]. Viruses are most easily 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 it's from and you are expecting it. Viruses can be disguised as attachments of funny images, greeting cards, or audio and video files. Viruses also spread through download on the Internet. They can be hidden in illicit software or other files or programs you might download.

2. How Computer Viruses Work

Strange as it may sound, the computer virus is something of an Information Age marvel [10]. On one hand, viruses' show us how vulnerable we are -- a properly engineered virus can have a devastating effect, disrupting productivity and doing billions of dollars in damages. On the other hand, they show us how sophisticated and interconnected human beings have become.

For example, experts estimate that the Mydoom worm infected approximately a quarter-million computers in a single day in January 2004. Back in March 1999, the Melissa virus was so powerful that it forced Microsoft and a number of other very large companies to completely turn off their e-mail systems until the virus could be contained. The ILOVEYOU virus in 2000 had a similarly devastating effect. In January 2007, a worm called Storm appeared -- by October, experts believed up to 50 million computers were infected [7]. That's pretty impressive when you consider that many viruses are incredibly simple. When you listen to the news, you hear about many different forms of electronic infection. The most common are:

Viruses - A virus is a small piece of software that piggybacks on real programs. For example, a virus might attach itself to a program such as a spreadsheet program. Each time the spreadsheet program runs, the virus runs, too, and it has the chance to reproduce (by attaching to other programs) or wreak havoc.

E-mail viruses - An e-mail virus travels as an attachment to e-mail messages, and usually replicates itself by automatically mailing itself to dozens of people in the victim's e-mail address book. Some e-mail viruses don't even require a double -click -- they launch when you view the infected message in the preview pane of your e-mail software.

Trojan horses - A Trojan horse is simply a computer program. The program claims to do one thing (it may claim to be a game) but instead does damage when you run it (it may erase your hard disk). Trojan horses have no way to replicate automatically [5].

Worms - A worm is a small piece of software that uses computer networks and security holes to replicate itself. A copy of the worm scans the network for another machine that has a specific security hole. It copies itself to the new machine using the security hole, and then starts replicating from there, as well.

Top threats

Worm:Win32/Sober.AH@mm
Exploit: Win32/Anicmoo.A
Worm:Win32/Nuwar.N@mm!CME711
Worm:Win32/Nuwar.N@mm!CME-711
Win32/Stration
Virus: W97M/Kukudro.A
Worm:Win32/Bagle.EG@mm
Exploit: Win32/Wordjmp
Worm:Win32/Mywife.E@mm
Exploit: Win32/Wmfap
Worm:Win32/Sober.Z@mm
Win32/Mytob
Worm: Win32/Mytob
Win32/Netsky

2.1. Virus, Worm and Trojan horse

The most common blunder people make when the topic of a computer virus arises is to refer to a worm or Trojan horse as a virus. While the words Trojan, worm and virus are often used interchangeably, they are not the same. Viruses, worms and Trojan Horses are all malicious programs that can cause damage to your computer, but there are differences among the three, and knowing those differences can help you to better protect your computer from their often damaging effects.

A ***computer virus*** attaches itself to a program or file so it can spread from one computer to another, leaving infections as it travels. Much like human viruses, computer viruses can range in severity: Some viruses cause only mildly annoying effects while others can damage your hardware, software or files. Almost all viruses are attached to an executable file, which means the virus may exist on your computer but it cannot infect your computer unless you run or open the malicious program [8]. It is important to note that a virus cannot be spread without a human action, (such as running an infected program) to keep it going. People continue the spread of a computer virus, mostly unknowingly, by sharing infecting files or sending e-mails with viruses as attachments in the e-mail.

A ***worm*** is similar to a virus by its design, and is considered to be a sub-class of a virus. Worms spread from computer to computer, but unlike a virus, it has the capability to travel without any help from a person. A worm takes advantage of file or information transport features on your system, which allows it to travel unaided. The biggest danger with a worm is its capability to replicate itself on your system, so rather than your computer sending out a single worm, it could send out hundreds or thousands of copies of itself, creating a huge devastating effect. One example would be for a worm to send a copy of itself to everyone listed in your e-mail address book. Then, the worm replicates and sends itself out to everyone listed in each of the receiver's address book, and the manifest continues on down the line [4]. Due to the copying nature of a worm and its capability to travel across networks the end result in most cases is that the worm consumes too much system memory (or network bandwidth), causing Web servers, network servers and individual computers to stop responding.

A ***Trojan Horse*** is full of as much trickery as the mythological Trojan Horse it was named after. The Trojan Horse, at first glance will appear to be useful software but will actually do damage once installed or run on your computer[3]. Those on the receiving end of a Trojan Horse are usually tricked into opening them because they appear to be receiving legitimate software or files from a legitimate source. When a Trojan is activated on your computer, the results can vary. Some Trojans are designed to be more annoying than malicious (like changing your desktop, adding silly active desktop icons) or they can cause serious damage by deleting files and destroying information on your system. Trojans are also known to create a backdoor on your computer that gives malicious users access to your system, possibly allowing confidential or personal information to be compromised. Unlike viruses and worms, Trojans do not reproduce by infecting other files nor do they self-replicate.

Added into the mix, we also have what is called a ***blended threat***. A blended threat is a sophisticated attack that bundles some of the worst aspects of viruses, worms, Trojan horses and malicious code into one threat. Blended threats use server and Internet vulnerabilities to initiate, transmit and spread an attack. This combination of method and techniques means blended threats can spread quickly and cause widespread damage. Characteristics of blended threats include: causes harm, propagates by multiple methods, attacks from multiple points and exploits vulnerabilities.

To be considered a blended thread, the attack would normally serve to transport multiple attacks in one payload [1]. For examplem it wouldn't just launch a DoS attack — it would also install a backdoor and damage a local system in one shot. Additionally, blended threats are designed to use multiple modes of transport. For example, a worm may travel through e-mail, but a single blended threat could use multiple routes such as e-mail, IRC and file-sharing sharing networks. The actual attack itself is also not limited to a specific act. For example, rather than a specific attack on predetermined .exe files, a blended thread could modify exe files, HTML

files and registry keys at the same time — basically it can cause damage within several areas of your network at one time.

3. Virus Evolution

As virus creators became more sophisticated, they learned new tricks. One important trick was the ability to load viruses into memory so they could keep running in the background as long as the computer remained on. This gave viruses a much more effective way to replicate themselves. Another trick was the ability to infect the **boot sector** on floppy disks and hard disks. The boot sector is a small program that is the first part of the operating system that the computer loads. It contains a tiny program that tells the computer how to load the rest of the operating system. By putting its code in the boot sector, a virus can **guarantee it is executed**. It can load itself into memory immediately and run whenever the computer is on. Boot sector viruses can infect the boot sector of any floppy disk inserted in the machine, and on college campuses, where lots of people share machines, they could spread like wildfire.

In general, neither executable nor boot sector viruses are very threatening any longer. The first reason for the decline has been the huge size of today's programs [2]. Nearly every program you buy today comes on a compact disc. Compact discs (CDs) cannot be modified, and that makes viral infection of a CD unlikely, unless the manufacturer permits a virus to be burned onto the CD during production. The programs are so big that the only easy way to move them around is to buy the CD. People certainly can't carry applications around on floppy disks like they did in the 1980s, when floppies full of programs were traded like baseball cards. Boot sector viruses have also declined because operating systems now protect the boot sector.

Infection from boot sector viruses and executable viruses is still possible. Even so, it is a lot harder, and these viruses don't spread nearly as quickly as they once did. Call it "shrinking habitat," if you want to use a biological analogy. The environment of floppy disks, small programs and weak operating systems made these viruses possible in the 1980s, but that environmental niche has been largely eliminated by huge executables, unchangeable CDs and better operating system safeguards.

E-mail viruses are probably the most familiar to you. We'll look at some in the next section.

3.1. Virus removal

One possibility on Windows XP and Vista is a tool known as System Restore, which restores the registry and critical system files to a previous checkpoint. Often a virus will cause a system to hang, and a subsequent hard reboot will render a system restore point from the same day corrupt. Restore points from previous days should work provided the virus is not designed to corrupt the restore files. Some viruses, however, disable system restore and other important tools such as Task Manager and Command Prompt. An example of a virus that does this is CiaDoor. Administrators have the option to disable such tools from limited users for various reasons. The virus modifies the registry to do the same, except, when the Administrator is controlling the computer, it blocks *all* users from accessing the tools. When an infected tool activates it gives the message "Task Manager has been disabled by your administrator.", even if the user trying to open the program is the administrator. If your system is a Microsoft product and you have your 20 digit registration number, you can go to the Microsoft web site, and they will do a free scan and most likely remove any known virus such as Trojan win32.murlo.

A program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes. Viruses can also replicate themselves. All computer viruses are manmade. A simple virus that can make a copy of itself over and over again is relatively easy to produce. Even such a simple virus is dangerous because it will quickly use all available memory and bring the system to a halt. An even more dangerous type of virus is one capable of transmitting itself across networks and bypassing security systems. Since 1987, when a virus infected ARPANET, a large network used by the Defense Department and many universities, many antivirus programs have become available. These programs periodically check your computer system for the best-known types of viruses. Some people distinguish between general viruses and worms. A worm is a special type of virus that can replicate itself and use memory, but cannot attach itself to other programs.

3.2. Virus Origins

Computer viruses are called viruses because they share some of the traits of biological viruses. A computer virus passes from computer to computer like a biological virus passes from person to person. Unlike a cell, a virus has no way to reproduce by itself. Instead, a biological virus must inject its DNA into a cell. The viral DNA then uses the cell's existing machinery to reproduce itself. In some cases, the cell fills with new viral particles until it bursts, releasing the virus. In other cases, the new virus particles bud off the cell one at a time, and the cell remains alive.

A computer virus shares some of these traits. A computer virus must **piggyback** on top of some other program or document in order to launch. Once it is running, it can infect other programs or documents. Obviously, the analogy between computer and biological viruses stretches things a bit, but there are enough similarities that the name sticks. People write computer viruses. A person has to write the code, test it to make sure it spreads properly and then release it. A person also designs the virus's attack phase, whether it's a silly message or the destruction of a hard disk.

There are at least three reasons. The first is the same psychology that drives vandals and arsonists. Why would someone want to break a window on someone's car, paint signs on buildings or burn down a beautiful forest? For some people, that seems to be a thrill. If that sort of person knows computer programming, then he or she may funnel energy into the creation of destructive viruses. The second reason has to do with the thrill of watching things blow up. Some people have a fascination with things like explosions and car wrecks. When you were growing up, there might have been a kid in your neighborhood who learned how to make gunpowder. And that kid probably built bigger and bigger bombs until he either got bored or did some serious

damage to himself. Creating a virus is a little like that -- it creates a bomb inside a computer, and the more computers that get infected the more "fun" the explosion.

The third reason involves bragging rights, or the thrill of doing it. Sort of like Mount Everest -- the mountain is there, so someone is compelled to climb it. If you are a certain type of programmer who sees a security hole that could be exploited, you might simply be compelled to exploit the hole yourself before someone else beats you to it. Of course, most virus creators seem to miss the point that they cause real damage to real people with their creations. Destroying everything on a person's hard disk is real damage. Forcing a large company to waste thousands of hours cleaning up after a virus is real damage. Even a silly message is real damage because someone has to waste time getting rid of it. For this reason, the legal system is getting much harsher in punishing the people who create viruses.

3.3. Self-modification

Most modern antivirus programs try to find virus-patterns inside ordinary programs by scanning them for so-called *virus signatures*. A signature is a characteristic byte-pattern that is part of a certain virus or family of viruses. If a virus scanner finds such a pattern in a file, it notifies the user that the file is infected. The user can then delete, or (in some cases) "clean" or "heal" the infected file. Some viruses employ techniques that make detection by means of signatures difficult but probably not impossible. These viruses modify their code on each infection. That is, each infected file contains a different variant of the virus.

4. How to Protect Your Computer from Viruses

You can protect yourself against viruses with a few simple steps:

If you are truly worried about traditional (as opposed to e-mail) viruses, you should be running a more secure operating system like UNIX. You never hear about viruses on these operating systems because the security features keep viruses (and unwanted human visitors) away from your hard disk. If you are using an unsecured operating system, then buying virus protection software is a nice safeguard. If you simply **avoid programs from unknown sources** (like the Internet), and instead stick with commercial software purchased on CDs, you eliminate almost all of the risk from traditional viruses.

You should make sure that **Macro Virus Protection** is enabled in all Microsoft applications, and you should NEVER run macros in a document unless you know what they do. There is seldom a good reason to add macros to a document, so avoiding all macros is a great policy.

Attachments that come in as Word files (.DOC), spreadsheets (.XLS), images (.GIF), etc., are data files and they can do no damage (noting the macro virus problem in Word and Excel documents mentioned above). However, some viruses can now come in through .JPG graphic file attachments. A file with an extension like EXE, COM or VBS is an executable, and an executable can do any sort of damage it wants. Once you run it, you have given it permission to do anything on your machine. The only defense is never to run executables that arrive via e-mail.

4.1. Firewall

A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria. There are several types of firewall techniques:

Packet filters: Looks at each packet entering or leaving the network and accepts or rejects it based on user-defined rules. Packet filtering is fairly effective and transparent to users, but it is difficult to configure. In addition, it is susceptible to IP spoofing.

Application gateway: Applies security mechanisms to specific applications, such as FTP and Telnet servers. This is very effective, but can impose performance degradation.

Circuit-level gateway: Applies security mechanisms when a TCP or UDP connection is established. Once the connection has been made, packets can flow between the hosts without further checking.

Proxy server: Intercepts all messages entering and leaving the network. The proxy server effectively hides the true network addresses.

In practice, many firewalls use two or more of these techniques in concert. A firewall is considered a first line of defense in protecting private information. For greater security, data can be encrypted.

4.2. Penetration Testing

Companies are increasingly turning to "penetration is testing" to evaluate the security of their systems on the Internet, contends Philip Whitmore. Also known as "white hat hacking" or "ethical hacking", penetration testing refers to evaluating the security of systems on the Internet by using the same techniques that are employed illegally by hackers. However, when used legally during penetration testing, these techniques are used in a more controlled and thorough way.

Unfortunately, given its rise in popularity and the benefits it offers, everybody is offering to do penetration testing. Don't be fooled – what one company may call penetration testing could be completely different to what another company calls it.

Companies seeking penetration testing services need to be aware of industry "cowboys" because they are out there – in all shapes and sizes.

Often what a client gets is nothing more than someone running a vulnerability scanning tool such as Nessus, Cybercop Scanner or Internet Security Scanner against an organisation's system and then giving a reformatted version of the output as the report.

Companies and organisations shouldn't be paying for someone to simply run a tool. Even worse, often the so-called penetration testing is no more than port scanning. Where is the value in that? Any IT person can pick up these tools and be proficient with them in a couple of hours. Simply running a vulnerability scanning tool is not a penetration test and sometimes it's worse than not doing

anything at all due to the false sense of security that may result.

Tools are just that, tools. A hammer doesn't build a house, the builder does. When used to supplement other work, the tools work well, but they are not particularly smart. Tools do not cover the range of possible weaknesses and generally do not provide comprehensive solutions or even, sometimes, ones that are correct.

It's surprising the number of times a report is produced where, for example, a Cisco router is being looked at with the finger service enabled, and the report states how to turn it off on a Unix system, not on a Cisco router. This is clear evidence that a tool has been run and not a lot else.

Real world experience is the key to effective penetration testing. Keeping up to date with security, new vulnerabilities, and techniques needed to effectively examine systems, is a full-time job requiring 100 per cent commitment from the people doing it. People who do this type of work part-time tend to have part-time knowledge.

5. Conclusion

Being largely misunderstood, viruses easily generate myths. Some people think it's funny to generate hoaxes. By careful checking you can usually spot them. Silly tricks and poor policies are no substitute for individual protection methods. Any product that advertises itself as a "quick and easy cure" for "all viruses past, present, and future" is more likely than not exercising its advertising imagination. Keep in mind that not everything that goes wrong with a computer is caused by a computer virus or worm. Both hardware and software failure is still a leading cause of computer problems.

Reference

[1] Kumar, Pankaj, "Computer Virus Prevention & Anti-Virus Strategy" (January 22, 2008). Sahara Arts & Management Academy Series Available at SSRN: http://ssrn.com/abstract=945758

[2] Mark Russinovich, Advanced Malware Cleaning **video**, Microsoft TechEd: IT Forum, November 2006

[3] Huntley C L, "A developmental view of System security", IEEE Computer Society, Vol 39, issue 1, Pg 113-114, Jan 2006.

[4] Jungck P, Shim ssy, "Issues in high speed internet security", IEEE Computer Society, Vol 37, issue 7, Pg 36-42, July 2004.

[5] Kemmerer R A, Vigna G, "Hi DRA: Intrusion Detection for internet Security", Proceedings of the IEEE, Vol 93, issue 10, Pg 1848-1857, Oct 2005.

[6] Kemmerer R A, Vigna G, "Intrusion detection: a brief history and overview", IEEE Computer Society, Vol 35, issue 4, Pg 27-30, April 2002.

[7] Sang Long Pao T, Po Wei Wang, "Net flow based Intrusion Detection System", IEEE international Conference on Networking sensing & Control, Vol-2, Pg 731-736, 2004.

[8] Sang Jun Han, Sung Bae Cho, "Evolutionary neural network for anomaly detection based on the behaviour of a program", IEEE Transaction on Systems, Man and Cybernetics, Part B, Vol 36, issue 3, Pg 559-570, June 2006.

[9] Chaker Katar, "*Combining Multiple Techniques for Intrusion Detection*", International Journal of Computer Science and Network Security, VOL.6 No.2B, February 2006.

[10] Geer D, "Behavior based Network Security goes mainstream", IEEE Computer Society, Vol 39, issue 3, Pg 14-17, March 2006.

Author's Biography

S.Jeya, has obtained her B.Sc., M.C.A., and M.Phill., degree from Manonmaniyam Sundaranar University in 1994, 1997 and 2004 respectively. She worked as Software Engineer at Bangaloor (1997-99) and Head of the MCA department at Rajaas Engineering College, Tirunelveli (1999-2006). Now she has been working as Assistant Professor in K.S.R. College of Engineering Tiruchengode, and pursuing her research work in Mother Teresa Women's University. Her interesting research area is "Network Security". Her research articles published in various International/National journals. She is a life member of ISTE, CSI.

Dr. K. Ramar, has obtained his B.E., M.E. and PhD degree in 1986, 1991 and 2001 respectively. He is working as Professor and Head of the CSE department at National Engineering College, Kovilpatti. He has more than 20 years of experience in teaching and research. He is also a member of various scientific and professional societies. His interesting research area is "Image processing" and "Network Security". His research articles published in various International/National journals.