Global Information Assurance Certification Paper

Cyber Threats: Viruses, Worms, Trojans, and DoS Attacks

Scott Hobbs

December 18, 2000

People are becoming cyber aware, now as computers and the Internet become part of people's daily lives and business. While using the Internet is becoming easier, so are the cyber threats and attacks to which people, companies, and groups are becoming exposed. There are many different types of cyber threats and methods to which to carry out the threats. Computer users, companies or individual web sites are vulnerable to cyber threats like viruses, Trojans, worms, and Denial of Service attacks. These common and often malicious threats need to be understood by anyone who has a computer. By understanding what the threats are and what they can do, users can better prepare themselves and their computers against the cyber threats.

One type of cyber threat comes in the form of Viruses. Viruses can be used to target a specific computer or they can be placed "in the wild" and make anyone with a computer a potential victim. A virus is "in the wild" when it is in the general public. Viruses are defined as files that are self-replicating, regardless whether it is malicious or not. Virus programs also require that the user activate them by opening the infected file, which launches the virus program. When the virus program is executed, one of its functions is to use the users e-mail application to replicate by sending itself to the addresses in the address book. If a virus is malicious, the virus program can have it take up space, delete the victim's hard drive, and/or delete or damage important files. The virus's design places the virus into three classifications of viruses; boot sector, file-infecting, and macro.

Boot sector viruses are platform dependent. This means that boot sector viruses can only affect specific hardware architecture. This virus mainly comes from infected floppy diskettes that are then used to boot to when the computer starts up. The virus is executed upon booting and then copies itself to the drive boot sector. From the time of infection and every time the computer is booted, the virus is loaded and can infect any new floppy diskette placed in the computer. Because boot sector viruses are platform dependent and rely on floppy diskettes as the way they are typically spread, they have become rare because people don't share floppy disks as much due to the Internet and electronic mail. A good precaution is to scan the floppy diskette with an anti-virus scanner that has updated virus signature files before booting from it, in order to prevent the virus from being loaded onto the computer.

The Internet has made file-infecting viruses very easy to spread. With the Internet, users can send more files and quicker than they could with floppy diskettes, thus making file infecting viruses a true cyber threat. File-infecting viruses also known as COM or EXE viruses, are platform as well as operating system dependent. They are easily spread through e-mails and any file transfer system. While file-infecting viruses are known as COM or EXE viruses, DLL, VxB, BAT, and HTML are some of the additional forms that viruses are currently being programmed with. These files need to be executed by the user, by launching the infected file. The virus then infects other files and depending on the program can continue to infect files or unload itself and repeat the infection cycle every time an infected file is executed again. The ILOVEYOU virus is an example of a file-infecting virus. The virus, written in VxB, overwrites .jpg and .mp3 files, sends a copy of itself to e-mail addressed in the victims address book in MS Outlook. A good precaution is to scan the executable with an anti-virus scanner that has updated virus signature files before executing the file.

Along with file infecting viruses, Macro viruses are a popular form in which viruses are being written in today. Macro viruses are application dependent, meaning that the virus can only run/affect the application the virus was written for. Microsoft Word, Excel, and PowerPoint, to name a few, are vulnerable to macro viruses written for them. The viruses are written to specifically exploit the macros in these applications. The macro is executed when the user opens an infected document in the appropriate application that uses the macro needed. The virus copies itself to the templates in the application, in order to infect future documents so when new documents are created they are infected with the macro virus as well. Besides scanning the file with an anti-virus scanner, a precaution that users can take is to not allow macros to be used in the applications. This will prevent the virus from being executed.

Similar to viruses but with a key difference are Trojans. A Trojan, also referred to as a Trojan Horse, may be or may not be a malicious program, that does something other than advertised or expected. Trojans are sometimes hidden with authorized programs or files and can be used to attack the victim at a later or predetermined date. Many Trojans are used to place remote access tools onto the victim's system to exploit the computer at the attackers will and without the user's knowledge. Trojans do require the user to initially open or run the virus

program. Once executed, the Trojan installs the code to carry out its designed, but unexpected, program. ExploreZip, is a Trojan that affects Windows systems and propagates itself in e-mail attachments. Once installed, the Trojan propagates and executes without any user interaction to other systems that are networked to the infected machine.

The characteristics that Trojans display, cross the line into another popular form of viruses, known as worms. Worms propagate through primarily through e-mail and mainly spread through a network. Worms are also file infectors or macro viruses that spread using MS Outlook. Unlike other viruses, worms do not need to be activated by a user or program in order for it to replicate itself. A worm is network aware and uses its awareness for its replication. A few examples of worms are W32/ExploreZip.worm and the Navidad Internet worm. These worms spread themselves through MS Outlook and change the registry of the infected computer. W32/ExplorerZip also targets other MS products, like MS Exchange and MS Outlook Express. While these worms concentrate on Microsoft products, any operating system or application is vulnerable to worms, but Microsoft is the most common operating system, so it is targeted the most. Just like with the other forms of viruses, Trojans and worms need to be scanned for. So the user should scan the files before executing them.

Denial of Service (DoS) attacks are a cyber threats that have to be specifically targeted, unlike viruses, worms, or Trojans. Basic DoS uses a single server to tie up a network's connection, deny users access to the targeted web site, or flood the server with useless emails with the purpose of bringing the server down. Distributed coordinated attacks (DDoS) use an unknown number of servers, or zombie systems, to attack the single server or web site. Using a DDoS disguises the attack, for the attack looks like legitimate attempts to access the server or web site because it comes from different sources, the zombie systems. Intrusion software cannot distinguish whether it is an attack or real connection attempt. Basic DoS attacks are possible to detect, with current software but very hard to prevent. This cyber threat can be easily carried out and accomplished with existing software and Trojans. Software is used to exploit holes in systems in order to gain control of them and Trojans are used to place remote access tools on systems for which the attacker can use to in the DoS attack, amking them zombie systems. In February of 2000, Yahoo, eBay, and CNN.com became victims of DoS attacks. The attacks either crashed the servers or slowed down access to the sites to the point that it disrupted business and created a major concern among people on the Internet. Just recently, due to the tensions in the Middle East, Lucent Technologies was attack by a DoS attack.

The characteristics of viruses, Trojans, and worms, blur the line as to what is specifically a virus, or a Trojan, or a worm. The ExploreZip virus has characteristics of a Trojan but also has the network awareness that might make it a worm. The Melissa virus is considered a macro virus since it exploits the macros in Microsoft Word, yet it too has network awareness to use Microsoft Outlook to send itself, thus making it a worm. Denial of Service (DoS) is another cyber threat that has characteristic of different types. While the basic DoS is not a Trojan, the Distributed coordinated attack (DDoS) uses systems that had Trojans place remote access tools on them and making available to be used in the DDoS attacks. While DoS is one type of attack, it incorporates other malicious programs in order to carry out the attack on the victim. As seen in the examples, malicious code writers use a combination of the different types to make the virus more effective and devastating.

Cyber threats are prevalent and devastating to systems, if they are infected, but there are preventative measures that can be taken to avoid becoming a victim. Simple security policies or procedures can be followed to protect computers. One is to use virus scanners that have updated virus signature files. This might take a concerted effort on the users part to keep the virus scanner updated but it is better than the alternative of being infected by a virus, worm, or Trojan. Never executing or opening unknown files is another procedure that should be followed in order to protect computers. Viruses and Trojan are dependent on unsuspecting users to open the infected files in order to activate the malicious code. So scanning and not opening unknown files will help prevent users from infecting their computer. Firewalls and intrusion detection software will help user protect their system from being taken advantage of or being used by others like in Denial of Service Attacks. Users cannot always keep the most determined attacker from infecting or using their system. But knowing what and how viruses, worms, Trojans, and Denial of Service attacks work, users will be aware of what they should and should not do to keep themselves and their computers relatively safe from cyber threats.

Sources

Gordon-Murnane, Laura. "Cyber-Threats: Protecting Against Computer Viruses with Alerts, Warnings, and Advisories." Searcher. July-August, 1999. URL: http://www.findarticles.com/cf_0/m0DPC/7_7/55144852/print.jhtml (5 Dec. 2000)

Hulme, George. "Lucent: Casualty Of Mideast Cyberwar?." TechWeb. 6 Nov. 2000. URL: http//www.techweb.com.wire.finance/story/INV20001106S0010 (4 Dec. 2000).

Lemos, Robert. "Cyber Attacks – Both Old and New." ZDNet. 20 October 1999. URL: http://www.zdnet.com/zdnn/stories/news/0,4586,2376768,00.html (5 Dec. 2000).

Williams, Martyn. "'Immense' Network assault takes down Yahoo." CNN.com. 8 February 2000. URL: http://www.cnn.com/2000/TECH/computing/02/08/yahoo.assault.idg/index.html (5 Dec. 2000).

"IT Security Focus Moves From Coders to Lawyers." Government Computer News. Volume 19, Number 32. 6 November 2000. Page 9.

"CERT Advisory CA-1999-04 Melissa Macro Virus." 27 March 1999. URL: http://www.cert.org/advisories/CA-1999-04.html (6 Dec. 2000).

"CERT Advisory CA-1999-06 ExploreZip Trojan Horse Program." 10 June 1999. URL: http://www.cert.org/advisories/CA-1999-06.html (6 Dec. 2000).

"Cyber-attacks batter Web heavyweights." CNN.com. 9 February 2000. URL: http://www.cnn.com/2000/TECH/computing/02/09/cyber.attacks.01/ (5 Dec. 2000).

"Information on the VBS/Loveletter Virus." Microsoft TechNet. URL: http://www.microsoft.com/technet/security/virus/vbslvltr.asp (23 May 2000).

"Middle East E-mail Flooding and Denial of Service (DoS) Attacks." National Infrastructure Protection Center (NIPC) – Warnings – 2000 Assessments. 26 Oct 2000. URL: http://www.nipc.gov/warnings/assessments/2000/00-057.htm (6 Dec. 2000).

"W32/ExploreZip.worm." Network Associates. 25 June 1999. URL: http://www.avertlabs.com/public/datafiles/valerts/vinfo/va10185.asp (6 Dec. 2000).

"W32 Navidad@M Worm." National Infrastructure Protection Center (NIPC) – Warnings – 2000 Assessments. 16 Nov. 2000. URL: http://www.nipc.gov/warnings/assessments/2000/00-059.htm