Author: Tyler Thomas

Website: www.SpaceAgeMinds.com

Last Revised: 5-2-10

Computer viruses, the potential dangers and unseen benefits

Computer viruses are programs with the power to spread to millions of computers and carry out a number of unwanted tasks. The Internet is the world’s first global network and it is open to everyone, every moment of the day. Because the Internet is open 24 hours a day a number of different viruses can be carrying out attacks on computers all around the world at any given moment. Viruses are written for a number of reasons but most virus programmers are motivated either by financial or technical gains. A discrete and professional programmer can make large amounts of money for designing and programming a virus. A lot of computer viruses do not seem that bad and will only send messages to the user as a joke, but the prank computer virus is a thing of the past. The most dangerous type of virus is financially backed, well programmed, and will infect millions of computers without giving the computer users the slightest clue. What most people do not realize about computer viruses is the extent of their destruction and their unseen benefits.

Most computer viruses are made by highly skilled individuals and sometimes commissioned by illegal organizations. Just as companies hire the best programmers to write their programs, illegal organizations also hire top programmers to write viruses. Computer viruses are made for a number of reasons. Some computer viruses are made as a proof of concept for research purposes’ but most are made for some sort of illegal activity whether it be to shut down a website through a disturbed denial of service attack or to steal personal information such as social security and credit card numbers off a victim's computer.

There are a number of ways for an illegal organization to make money from a computer virus. One of the main ways virus programmers make money is by sending out massive amounts of spam from its infected computers. In the article *The Worm That Roared* the author Lev Grossman details the computer super virus known as “STORM”. He explains how “back in the day, computer viruses were a relatively innocent affair, written as pranks by teenagers with too much time on their hands between Star Wars sequels. Now they're written by organized criminals looking to make money from fake offers” (Grossman 2). Today's virus writers are motivated by financial incentives, whether it is by sending out massive amounts of spam email with fake offers or stealing your personal information and selling it. In the article *Controlled Chaos* the two authors, Antonio Nucci and Steve Bannerman, also talk about the virus “STORM” and how it “methodically infiltrates computer with dormant code that could be used to take down the entire network of a corporation, creating opportunities for blackmail or for profiting by selling the company's stocks short”(Bannerman 44). With the flip of the switch STORM's programmers could hold an entire company hostage. With on line companies like Amazon.com and Ebay.com a couple days of downtime can result in millions of dollars lost.

Computer viruses are some of the best designed programs ever written. The goal of computer viruses is to spread to as many computers as it can and run computer code without being detected. A well designed virus is able to spread across the Internet undetected and plant itself on millions of computers around the world. When a virus is on a computer it scans and sends out multiple copies of itself or it waits for an incoming command. In their article *Striking Similarities* Frederic Perriot, Peter Ferrie, and Peter Szor give a sense of how complex viruses can be by talking about the "Win32/ Simile" virus. The authors say "Win32/Simile moves yet another step up the scale of complexity. The source code of the virus is approximately 14,000 lines of assembly code. About 90% of the virus code is taken up by the metamorphic engine itself, which is extremely powerful"(Perriot 1). It is assumed that the Win32/Simile virus was written as a proof of concept because it's only payload was to display a message on a specific day and did nothing specifically harmful to the user's computer. The virus' main feature was its metamorphic engine which rewrites and encodes the viruses each time it is sent out. This metamorphic feature makes the virus extremely hard to detect because each instance of the virus was unique. With such sophisticated code viruses are able to spread extremely fast and are increasingly difficult to detect.

Viruses are able to spread in a number of ways. In the article *Controlled Chaos* the two authors go into detail about how "Storm is far more sophisticated than previous worms, because it uses peer-to-peer technologies and other novel techniques to evade detection and to spread" (Bannerman 43). Once a virus has avoided an anti virus program and infected a computer through one of its many modes of transmissions it either uses that computer to spread and infect more computers or it carries out an attack. In the same article the authors explain a denial of service attack,

> *"In order to maximize the mayhem, attackers spread out there attacks by hijacking unprotected machines on the internet and planting code that*

> *recruits them as "zombies" (or "bots," short for robots). These computer in effect form armies ("botnets") that number in the tens of thousands and can be orchestrated to launch attacks that emanate from multiple sources" (Bannerman 45).*

Having that many computers at their disposal allows the attackers to shutdown any website they want. By commanding the "zombie" computers to repeatedly request information from a website the attacker overloads the web-site's severs which forces the website to shuts down.

Computer viruses have a number of potential targets. Any number of infrastructures that relay on the Internet including large companies, banks, and even different world governments are at risk of being a target. Large Companies are one of the main targets for virus attacks. Companies can be targeted for a number of reasons by a number of different groups, not just hackers trying to make money. For example an American pharmaceutical company, Abbott Laboratories, was attacked by Act Up/Paris which is a French group of AIDS campaigners. The group used a distributed denial of service attack to take down Abbott Laboratories' website in protest of Abbott overcharging people in poor countries for AIDS medications (Economist 1). Viruses allow groups from around the world to take action against any major foreign company for whatever the reason may be. The effects range from website downtime to millions of dollars lost in on line sells or data center repair.

Another target for attacks by computer viruses is banks and their customers. Virus creators are using America's current financial crisis to their advantage. In Matt Hines security watch commentary entitled *Is economic turmoil really driving Threats?* He point out that "in the first quarter of 2008, Cyveillance, a private internet-monitoring company, reported that it saw an average of roughly 400 attacks per day. However in the past month, the firm has seen an average of more than 1,750 campaigns per day with some record-level days where attacks numbered as many as 13,209"(Hines). Virus creators are using this situation to their advantage by increasing the number of attacks on banks and trying to get bank specific information from customers.

An example of a virus playing a major role in government affairs was the 2007 Cyber attack by Russian hackers on the Eastern European country of Estonia. In the article, "A good bot roast", the journal *Economist* examined the attack and looked at its economic impact. It talks about this attack and calls it "a danger to national security, the national information infrastructure, and the economy" (Economist). The attack, which was carried out by a number of Russian Hacker groups, clogged Estonia's Internet arteries by sending massive amounts of fake traffic from bot-nets located around the world to its networks which "attracted close attention from NATO, the Pentagon and other government agencies" (Economist). Banks, Government, and E-commerce web resources were closed for days and as a result Estonia's economy was hugely affected.

Computer viruses will not go away and are essential in the development of future Internet technologies. The *Merriam-Webster dictionary* defines a virus as "the causative agent of an infectious disease", this definition holds true for computer viruses as well. A virus infects a user's computer without warning. Just as your body develops responses for viruses, the Internet and it's nodes responds to viruses and their inherent threats through software and hardware updates. Because of the constant attacks from viruses, software and hardware vendors are forced to update and improve their products on a regular basis because new software tends to be less vulnerable then old versions. Viruses are also changing the way computer scientist program. Due to the large number of virus attacks each day computer programmers are forced to think about security when writing new programs.

With the power to spread to millions of computers undetected computer viruses are an extreme threat. Because the Internet is open 24 hours a day computer viruses can strike at anytime. Motivated by money a discrete and professional programmer can make large amounts of money for engineering and programming a well designed virus which can attack from anywhere in the world. The most dangerous type of virus is financially backed, well programmed, and will infect your computer without even being noticed. What most people do not realize about computer viruses is the potential extent of their destruction on the world's infrastructures. If you were to ask an average American where the most likely place for the next major terrorist attack, they would most likely say San Francisco, The Pentagon, or any other major city or government building. The real danger is on the Internet creeping into computers without being noticed getting ready to strike hospitals, 911 call centers, and financial companies. There is also an unseen benefit to all of this. Because viruses can come from anywhere at any time technology companies can never let their guard down. They are constantly upgrading, repairing, and creating new software and hardware all the time.

Works cited

"A good bot roast." Economist 383.8534 (23 June 2007): 68-68. Academic Search Premier. EBSCO. 9 Dec. 2008 http://proxy.lib.csus.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=512502&sit

Bannerman, Steve and Antonio Nucci. "Controlled Chaos." IEEE Spectrum December (2007): 43-48.

Perriot, Frédéric and Péter Ször, Peter Ferrie. "Striking Similarities." VIRUS BULLETIN May (2002): 4-5.

Hines, Matt "IS ECONOMIC TURMOI! REALLY DRIVING THREATS?" eWEEK December (2008): 50.

Grossman, Lev. "The Worm That Roared." Time 170.15 (08 Oct. 2007): 68-69. Military & Government Collection. EBSCO. [Library name], [City], [State abbreviation]. 18 Dec. 2008 <http://proxy.lib.csus.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=mh&AN=26882299&site=ehost-live>.

Merriam-Webster dictionary. "Virus"