Steven Lindstrom

COM 1101

Dr. Perdigao

12/9/2004

Malicious Code Maliciously Misunderstood

When the word "hacker" is mentioned, a negative connotation almost immediately comes to mind, largely due to the misuse of the word. A computer hacker is merely a person who is an expert at anything involving computers, be it programming or using hardware, because it is a hobby (Harvey). The definition that most people wrongfully give hackers is that of a cracker, which is a person that uses his/her knowledge of computers for less honorable intentions, like password theft, information theft, or just wreaking havoc in cyberspace (C.N.N.S.L.). Another catch-phrase that is also slandered with a negative implication is "malicious code." Malicious code is most commonly thought of as viruses and is also most commonly, and wrongfully, associated with hackers. However, by definition, malicious code is anything included in a system for an unauthorized purpose (C.N.N.S.L.). Despite these misconceived viewpoints on the subject, malicious code should continue to be written since it is not necessarily all that bad.

Every time a computer slows down or does something that the user considers "funny," he/she uses all of his/her deductive computer skills to analyze the problem, ultimately deciding that it must be a virus or something to that effect. Sometimes this is true, but most of the time this is simply not the case. It is fairly safe to say that the majority of people do not know how to properly care for their computers, and this is what truly makes them slow down or act "funny." Proper maintenance that takes around five minutes to perform can keep a computer running like it is brand new.

For example, most people do not delete their temporary internet files, which can take up a significant amount of memory, depending on the last time they were deleted. Basically, temporary internet files are copies of web pages and images found on the web pages that were viewed by the user. They are not really bad because the next time the user goes to one of these sites, it will load much faster. However, without regular deletion, these files can slow the computer down significantly. Another common step to maintaining a healthy PC that most do not do, is defragmenting the computer's hard drive. When a computer modifies or deletes files, it stores part of the file on a different place on the hard drive, depending on where the closest free space is. With parts of files scattered about the hard drive, it takes more time for the system to load these files since it takes longer for it to find all of the pieces. The only way to combat this is to use a system tool called the "defragmenter." All this tool does is place the various parts of files all together, resulting in reduced loading time. The last, and probably most import step to proper computer maintenance is turning the system off properly. When the user simply holds the power button until the computer shuts off, this can harm or even destroy the operating system. This is because when the system is properly shut down, the computer saves certain files, tells others to stop running, and then shuts the power off. If the power is immediately shut off, files can be damaged or even deleted.

When a computer is actually infected by malicious code, it is more common for it to be infected by spyware, which, according to the University of Central Florida, is "[a] technology that assists in gathering information about a person or organization without their knowledge" (Pegasus). However, there are different kinds of spyware. The most common form is known as a cookie. Cookies are data files saved on computers by websites that contain information about the user. While this sounds threatening, cookies are really there to help. Often times they

remember passwords so the user does not have to retype them, preferences so the user does not have to reselect them, or even items placed in a virtual shopping cart so that the user does not have to buy multiple items in individual transactions. Like anything else in a computer, cookies take up space and occasionally need to be deleted, but the more harmful type of spyware is the kind that embeds itself into a computer without the user's knowledge. From this point, spyware can be further broken down into a few categories. One kind of spyware does just what its name implies; after self-installation it spies on the user, gathering information about him/her and reports its findings to whoever created it. After the information is sent back, it is usually sold to vendors that will send information about their product via e-mail or various other methods. The other kind of spyware, which is most commonly mistaken with viruses, is the kind that sends pop-up advertisements to the user's screen, with the intent that the user will click on the advertisement and purchase some product. Both forms can be fairly hard to remove, but with Microsoft Windows XP or 2000, there is a free firewall available to users that can block most forms of spyware. Simply put, a firewall is a program that monitors all of the information traveling to and from your computer at any given time and gives the user the option of selecting what information will be allowed to pass through. In addition to the Windows firewall, there are many other free firewalls that work with most operating systems. For the few instances of spyware that slip through, though, there are free programs that scan for the files and then remove them.

The preceding demonstrates how malicious code is most commonly confused with improper maintenance, however, when it actually comes to malicious code in the form of viruses it is a totally different game. While most viruses should be caught by the computer's anti-virus tool, this is not always the case for several reasons. The most common reason that viruses are

able to infect an average person's system is because the anti-virus tool is used improperly. Most anti-virus programs analyze incoming data and compare it with a virus database, or "virus signatures," and if the data matches, an alert warns the user about a virus (de la Cuerda). Others can detect if the incoming data has the potential to do hazardous things and will warn the user if so, irregardless of whether it contains a virus or not (de la Cuadra). However, if the user never updates the anti-virus tool's virus database, the program will not know to look for the new viruses that are developed daily. The other most common reason for virus intrusion on a person's computer is that the user unleashed the virus by opening a certain file. When it comes to opening files, it is good practice to know what the file is, where it came from, and what it does. If the user does not know the answer to any of these questions, the file should either be scanned by his/her anti-virus tool, or not opened at all.

Since the Internet was created, there has been quite a history of viruses. Viruses are commonly found on the Internet in places that most should probably avoid; pornography sites, warez sites (sites that provide stolen programs), or even on peer sharing programs, like Kazaa, Napster, and LimeWire. In May 2000, the biggest computer virus outbreak in history occurred when Onel de Guzman unleashed the "I Love You" virus on the world, resulting in more than eight billion dollars of damage (Zetter). After being brought to court, the charges against Guzman were dropped because of the absence of virus distribution laws in the Philippines, where he resides (Zetter). Another famous court case is that of a man who did nothing nearly as serious as Onel de Guzman. In 1999, Peter D. Junger, a professor at Case Western Reserve University in Cleveland, was brought to federal court because he tried to post the source code to an encryption program he had written on his web page to help his students learn (Mendels). The government views encryption, or the of scrambling data to keep it secret, as a matter of national security, but

Junger felt that his Constitutional rights were being violated (Mendels). After the first federal ruling that deemed that source code was not protected by the First Amendment, Junger brought his case to the Supreme Court (Mendels). After this trial, the Supreme Court ruled that computer source code is protected by the First Amendment because it is "...an expressive means for the exchange of information and ideas about computer programming... (SAMSARA)." Even though malicious code has the potential to do harm, the 1969 Supreme Court case Brandenburg v. Ohio ruled that violent speech, which can now be applied to malicious code, is only illegal if it is written in such a way that it calls for actions to be done that create an immediate apprehension of fear (Bomb Recipes). So, because of this ruling, writing malicious code or detailed instructions on how to write it is viewed as being perfectly legal. The reasoning behind this is that the author has no idea who will read his/her work, and therefore cannot be held responsible for the actions of others (Bomb Recipes).

Because the writing of malicious code is clearly protected by the First Amendment, it cannot be made illegal, unless the First Amendment is changed or ignored. Executing code, on the other hand, could potentially be made illegal, although it should not be. The reasoning behind this is that with shoddy definitions of malicious code, it would then become possible to make most software illegal, thus setting the computer age back severely. Since most people do not have such an in depth knowledge of computer programs, how they are written, or even what their specific functions are, it would be very easy for an unqualified lawmaker to outlaw malicious code. Even if it was made illegal, malicious code would continue to be written by some anyways. After all, murder is illegal, and yet the murder rate is still very high in certain areas. In this scenario, malicious code would still be running wild, but there would be no software to counteract it because it would be illegal to have malicious code saved in an anti-virus

program.

In addition to this, with all ethics put aside, malicious code should not be banned because there is so much that can be learned from it. Because of malicious code, security breeches are discovered in software nearly every day. With more security breeches, software will begin to get more secure and require fewer updates. For example, Microsoft releases patches for Windows nearly every week. Had these flaws been known before releasing the software, these updates would not be necessary. If people write malicious code in a controlled environment to try to break a program, or get around an anti-virus program, they need to look at things differently; more like a devious cracker using all of his/her skill to complete a single objective. With this viewpoint applied to the development and testing of new software, holes in security are bound to disappear. Also, writing malicious code may lead developers onto a new algorithm for solving a certain problem. Since the number of solutions to problems is limitless, that means that many different things can come to similar conclusions. What if, by chance, a new use was found for malicious code, or even just a few lines from malicious code? Although it has probably been done before, this would be a step in the right direction for people to apply their knowledge in a positive way in regards to the subject.

As can be seen, malicious code is a major part of the computing world in large. It's creation will never stop, and neither will its execution no matter what laws are put in place to combat such actions. Aside from being an occasional annoyance found when illegally downloading music, malicious code is not as rampant as many are lead to believe. Malicious code has been around since computing first began, and the majority of people have learned to live with it. Like illness, malicious code requires certain precautions to prevent being affected by it. Anti-virus software and firewalls, both of which can be found free of charge, can

and will put the advantage in the user's hands, thus making it possible to enjoy Internet access without apprehension of contracting viruses or spyware. The only other option that will guarantee that a computer will not be infected by any malicious code of any sort is to never plug the computer into a network of any kind and never add anything to the computer. Since the latter is not of much desire to most users, it is reasonable to say that in this day and age, it is absolutely necessary to own a firewall and some kind of anti-virus software. This situation may change in the future, but until then the state of computer security is infinitely unpredictable.

Works Cited

"Bomb Recipes." The Ethical Spectacle: The Museum of Free Speech. 30 Nov. 2004 <http://www.spectacle.org/freespch/musm/bomb.html>.

C.N.N.S.L. Glossary. 15 Oct. 2001. Texas State Library and Archives Commission. 30 Nov. 2004 <http://www.tsl.state.tx.us/ld/pubs/compsecurity/glossary.html>.

de la Cuadra, Fernando. "How anti-virus programs work." The British Computer Society. 14 Dec. 2004 <http://www.bcs.org/review04/articles/itsecurity/virus.htm>

Harvey, Brian. "What is a Hacker?" Computer Science Division, University of California Berkley. 30 Nov. 2004 <http://www.cs.berkeley.edu/%7Ebh/hacker.html>.

Junger, Peter. "Samsara's Web Server." Case Western Reserve University. 30 Nov. 2004 <http://samsara.law.cwru.edu/>.

Mendels, Pamela. "Professor Argues for Free Speech in Computer Tongues." The New York Times 5 Mar. 1999. 30 Nov. 2004 <http://www.nytimes.com/library/tech/99/03/cyber/cyberlaw/05law.html>.

The Pegasus Disc: Glossary. University of Central Florida. 14 Dec. 2004 <http://www.tsl.state.tx.us/ld/pubs/compsecurity/glossary.html>.

Zetter, Kim. "Freeze! Drop That Download!?" pcworld.com 16 Nov. 2000. 14 Nov. 2004 <http://www.pcworld.com/news/article/0,aid,34406,00.asp>