Global Information Assurance Certification Paper

Robert Woods
March 15, 2004

Security for the Average Home PC user
Virus protection

GIAC Security Essentials Practical

Abstract: This paper has a purpose of security education. The target audience is the average home PC user as stated in the title. Most home users are just now grasping the technology and have no concern about security. That is a nightmare to corporate America and themselves. In order to be approachable to a mostly non-technical audience this project is written in very plain, easy to understand English yet dives right into the explanation of viruses and how to protect against them using anti-virus software. An introduction or plea to the audience starts the paper off followed by a short history of secure computing. Since there is a common ignorance about the types of threats that exist the next section is devoted to defining the different types of computer viruses and information that most of us Security Analysts probably take for granted. After explaining the threat the average user needs to understand what is being done and where they can go to get more information. Section 3 covers the tools people can use to fight this security battle and speaks about efforts to slow down the growing threats. Finally, there is a short list of resources that even the beginner can digest.

If you are reading this then it no doubt means that I was able to convince the folks at GIAC that one of the most important things involving secure computing is education. Well they already know that because in many ways they are in the business of security education. Typically this type of project would be very technical and as such geared toward a more technology savvy group. I am presenting that type of information but will attempt to do it in a way that anyone can understand. As a security analyst I get to work with many different types of security tools and cutting edge technologies and hopefully I can share that information with others in need. My job is to try and keep the bad guys out or at least slow them down enough where they get bored and decide to pick an easier target. Make no mistake about it that if someone wants to penetrate your network or home computer it can be done. The only way to really keep attackers from getting you is to not be connected to the outside world. Further, one of the most frightening things is how big a threat hackers pose when they are organized. There are organized crime groups who have been able to gather thousands of computers, known as zombies or bots, and install programs that will execute attacks against specific targets. The latest of this type of attack is happening presently against a software provider known as SCO. The creators of the MyDoom virus have been able to spread their infected program to thousands of machines. The program was written to spread and then launch a distributed denial of service (DDOS) attack against SCO. Did it work? It absolutely did. The company had to bring up a temporary Internet site because this attack was able to completely block their website. How did the attackers do this? They took advantage of people. They created a virus that was attached to an email that looks legitimate. When you click on the email the program executes and installs on your computer. Then it looks for email addresses you have stored and sends copies to all of your friends and family. Security analysts know all about this stuff and I hope that even the average user will have the same passion to protect themselves as analysts do. With this type of threat looming there is nothing that would stop a hostile nation from attacking our government systems. There is a never ending list of possibilities so please take action to help stop these threats. If you don't understand after reading this paper find someone who can help. If you are an analyst who knows this material then start sharing the information with your less knowledgeable friends, family and neighbors. On with the presentation.

I. State of Computer Security and History of secure computing.

So why should you care about securing your computer? Would you like the short answer or the laundry list? It may not even be possible to give a short answer except to maybe state that everyone is vulnerable to threats today if you access the Internet using a PC. In reality the threat is even broader than that. To understand the importance of security it is absolutely necessary to look at how our world has changed because of the computer. In an effort to spend more time focusing on how to secure your electronic resources this State of Computer Security and history of secure computing will be brief. After this is

explained then the focus will shift to defining in more detail the nature of the threats and how everyone is vulnerable. This is not a tragedy though as the last part of this paper will be geared towards helping anyone and everyone protect themselves from the evil doings that is cyber crime. Before a brief history here is a wake-up call. "It's early in 2004 and Microsoft is sick with nearly 65,000 viruses, it's crawling with worms, and there are enough packaged Trojans sitting around to wreak havoc on almost any virile computer."[7] These and other security terms will be defined throughout this project.

The difficult part is where to start. Really understanding secure computing requires a history lesson. Early computers were developed as a means of storing information. When computers first surfaced they were bulky, expensive and not realistic for public use. Because of the limited technology and knowledge base security concerns were mainly preventing people from gaining physical access to the equipment. As technology slowly improved the amount of information and types of data being stored and referenced began to change. Because of this there was a desire to share information between more than one location. The birth of the Internet was now on the horizon. The government and large companies continued to develop more complex networks in order to share information. These networks started to connect and before long businesses understood the potential of online business. Improvements in technology made computers smaller and cheaper. Now PC's started popping up in homes and at schools. The Internet now had a foundation and just exploded. Companies started offering products and services online. People actually communicated via email more than written mail. With all of these electronic communications and explosion of technology the threats to companies and individuals also grew. Now just locking the huge computer systems in a room away from everyone was not adequate protection. Computers were not much more accessible and people had to start thinking about how to electronically lock out the bad guys since so much information was being shared over the wire. That brings us to the mess we have today. The downside to all of this is that the average user is just now grasping the use of the technology and thinks nothing of securing their information.

One of my favorite Security columnists put it all in perspective recently in one of his articles. "Security is just not a concept that "normal" folks focus on. It's not even on the radar screen. It's just not thought about at all."[4] It is my desire that you, "the average PC user," will at least increase your awareness of these threats enough to search for more information and help.

II. Understanding the threats

Now it is necessary to understand what the risks we all face are. Computer viruses are something we may have heard about but do not always understand. That ignorance contributes greatly toward keeping the majority of

PC users vulnerable. If someone does not understand what the threat is then they do not know how to defend against it. I will discuss the most common types of viruses and how they can infect. Security Analysts understand this in the most intimate details but this is meant for all to understand.

Computer Viruses

One of the most common types of cyber crime or abuse that affects almost all of us is computer viruses. So let's take a look at computer viruses and understand what they are and how they affect us. Webster's dictionary defines a computer virus this way: A computer program that copies itself into the other programs stored in a computer with either a benign or negative effect.[8] Well thanks for the assistance. That doesn't really clear anything up for anyone. Many would use a human virus as an analogy to explain what a computer virus. Marshall Brain did exactly that in an informative article on the website www.howstuffworks.com titled "How Computer Viruses Work." Brain explains.

> 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.
>
> There are similarities at a deeper level, as well. A biological virus is not a living thing. A virus is a fragment of DNA inside a protective jacket. Unlike a cell, a virus has no way to do anything or to reproduce by itself -- it is not alive. 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 get executed. Once it is running, it is then able to 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.[1]

There are thousands and thousands of viruses but most fit into a few generic categories. A *file virus* is one that infects applications. When the infected application is opened or executed the virus spreads by infecting associated documents and then spreads to other applications. Another type of virus is known as a *boot sector virus*. This gets its name by how it infects a computer. This type of virus infects the first sector of a disk drive known as the boot sector. This can keep your computer from booting up depending on how the virus code is written. Probably the most common type of virus is called a *macro virus*. One of the virus information sites I recently visited estimates that 75% of the viruses found in the wild are of this type.[2] These viruses affect

Microsoft Office applications such as Word and Excel. There are other types of viruses but the one that gives anti-virus protection the biggest challenge is called a *polymorphic virus*. The reason that this type of virus is such a challenge is that each new copy of the virus looks different than the last. Fortunately for the security industry this type of virus looks better on paper than in reality.

Now we know why they are called virus we have a little better grasp on why we should be concerned about the spread of this pest. Just like human viruses their computer counterparts come in many flavors and some are more harmful than others. The next couple of sections are meant to shed a little more light on the common infection methods for computer viruses.

Email Virus

An email virus gets its name by the method it uses to infect others. You guessed it this variety uses email as a bridge. This program can spread very fast because the program is written to actually go in and search your email addresses and then send copies of the infection to everyone in your address book. The two most common email viruses in recent times were the Melissa and ILOVEYOU viruses. Both of these were very tricky. Tricky in that they both took advantage of trust to allow for the virus to spread. Melissa was created using something very common and well known to the standard PC user, a Microsoft document. This program was written with a friendly message with the receiver's name and looked absolutely trustworthy. Then when the unsuspecting victim opened the document the virus program went to work. The first thing the virus did was collect names from the email address book and send copies of itself out to other people. It sounds pretty harmless and even a little humorous. In fact this was one of the fastest spreading email viruses to date and harmless it was not. Many companies had to completely shut down their email systems. That is huge in a time where many of us rely heavily on communicating electronically and cost many corporations millions of dollars.

Worm

So is this something that crawls into my computer and eats the insides? Well not literally but if you think about it that is close to reality. Most of the time there is no way of predicting how much or fast a worm might spread. This type of virus is usually written to take advantage of some type of known vulnerability. That is to say that these virus programs spread because of some type of weakness found in an application or operating system. Blaster, Code Red, SoBig and the Slammer worms are all great examples of malicious worms. All of these viruses had evil intent and the authors knew that there was potential for a large scale effect. This type of virus has caused many software manufacturers to reevaluate the priorities on their product offerings. The latest beast from this category seems to be one of the worst according to many analysts. Mydoom hit the scene in late December 2003 early January 2004 and wreaked havoc. These viruses have had a terrible effect on individuals and large corporations alike.

Trojan horse program

Some people don't consider a Trojan horse program a computer virus. I felt inclined to include it in this section because it is a program that sometimes contains viruses. Trojan horses also serve other purposes to an attacker such as installing back doors for remote access. Trojan horses are one of the purposes the previously mentioned viruses are designed. Much like the giant wooden horse given to Troy that seemed a good natured symbol of friendship a Trojan horse program is something that looks innocent enough. These programs are usually disguised as something useful to the average user or entertaining like a computer game. When the unsuspecting person downloads and installs the program they get more than they bargained for. More likely than anything the actual Trojan horse program contains a virus or some type of remote access program allowing attackers access to your system. A recent report showed that someone was actually jailed for child pornography because of a Trojan horse. Lucky for him after some investigation the person was found to be innocent. "A man has been cleared of child porn charges, after investigators found that an Internet attacker was responsible for the presence of illicit images on his PC."[3] You guessed it a Trojan horse was found on the victim's computer. The attacker used the compromised machine to surf and store child pornography without being detected. These programs are no joke folks. The article explains more about Trojan horse programs and the grave danger they pose to us all.

Anti-virus software vendors offer a lot more information on their websites about virus characteristics. Type of propagation, attachment type, registry keys and removal instructions can usually be found about every type of virus in the wild. Check out the resource list at the end of the paper for more information regarding viruses and the removal solutions.

III. What can be done?

There are many things that even the most technology challenged of us can do that can make a difference. Once you understand the threat it is easier to find ways of making yourself less vulnerable to attacks. Anti-virus software is a must if you connect to the Internet and we must practice secure computing. Even the State and Federal government as well as large corporations are making efforts to help prevent these attacks.

Anti-virus (AV) software

Scanning Software

If you do not have anti-virus software get some now. Many of the worst viruses that are known today can be prevented by installing and properly maintaining anti-virus software. Maintenance is important also because when

new viruses are written the companies who develop this software release definitions of the virus so your software can detect and prevent the virus. Symantec, McAfee, Trend and Sophos are just a few of the many companies who offer anti-virus software to the individual user. The websites for these companies are listed in the last section of this paper. Besides these vendors there are actually free versions of anti-virus software available with a little research.

What is anti-virus software and how does it work? That is a great question and needs to be answered to help us understand the important function it serves. First of all I would like to point out that it is imperative that anti-virus software is kept up to date. If we use the same comparison as before, anti-virus is to a computer virus what antibiotics are to a human virus. The following will describe how anti-virus software works.

The 2 main parts to anti-virus software are the scanning engine and virus definitions. The *scanning engine* is the part of the software that actually checks your computer for virus information. This is very flexible in that you can set up the software to scan all incoming documents on the fly, schedule scans of your file system or manually scan your system. The second part of anti-virus software is the *virus definitions*. Now the unfortunate part about anti-virus protection is that we must actually analyze the virus code before we can design virus definitions. That means that protection against viruses is usually after a virus has already infected many computers. This also means that it is very important that we keep on top of updating our software regularly. So the basic idea of how the software works is the scanning engine scans all the files on your computer and searches for specific strings of information that create a sort of footprint. This footprint information is what makes up the virus definition file.

Even though this type of software is available free the support for free software in reality is non-existent. It is highly suggested that if possible people purchase anti-virus software from a trusted vendor that has the resources to publish virus definitions quickly.

Fix tools

One of the things that is becoming very common with recent virus outbreaks is what is known as fix tools. These are very similar to scanning software in that they use a scanning engine and virus definitions to search your computer for a virus. There are a few differences though. These fix tools are developed using the same type of scanning engine but they are much smaller because they are designed to look for only one virus. That is right they only have one virus definition. There is another difference too. A virus has certain things it executes on our computers. The virus usually leaves an executable file on our computer but it may also make changes to our registry or other system resources. The fix tools are written to include this type of information in the virus definition. The fix tool not only identifies the infected files and virus itself but it does what the name implies, it repairs things. These fix tools are usually posted on Anti-virus companies web sites and are free to download. I have personally found them very helpful and used them as recently as the outbreak of the

W32.netsky.C@mm virus. I had a relative that clicked on an attachment which contained the virus. The virus took up all of her processor just trying to send out copies to all of the email addresses it could find. Because of this she was not able to get to her anti-virus vendor's web site to download new virus definitions. The only way we could get her small business back on line was to use a fix tool. Following is some information of what a fix tool does:

W32.Netsky@mm Removal Tool

Symantec Security Response has developed a removal tool to clean infections of the following Netsky variants.

- W32.Netsky.B@mm
- W32.Netsky.C@mm
- W32.Netsky.D@mm
- W32.Netsky.E@mm
- W32.Netsky.K@mm

What the tool does

The W32.Netsky@mm Removal Tool does the following:

1. Terminates the W32.Netsky@mm viral processes
2. Deletes the W32.Netsky@mm files
3. Deletes the registry values that the worm added

Available command-line switches for this tool

Switch	Description
/HELP, /H, /?	Displays the help message.
/NOFIXREG	Disables the registry repair (We do not recommend using this switch).
/SILENT, /S	Enables the silent mode.
/LOG=<path name>	Creates a log file where <path name> is the location in which to store the tool's output. By default, this switch creates the log file, FxNetsky.log, in the same folder from which the removal tool was executed.
/MAPPED	Scans the mapped network drives (We do not recommend using this switch. See the following Note).
/START	Forces the tool to immediately start scanning.
/EXCLUDE=<path>	Excludes the specified <path> from scanning (We do not recommend using this switch. See the following Note).

Note: Using the /MAPPED switch does not ensure the complete removal of the virus on the remote computer, because:

- The scanning of the mapped drives scans only the mapped folders. This may not include all the folders on the remote computer, which can lead to missed detections.

- If a viral file is detected on the mapped drive, the removal will fail if a program on the remote computer uses this file.

Therefore, you should run the tool on every computer.

The /EXCLUDE switch will only work with one path, not multiple. An alternative is the /NOFILESCAN switch followed by a manual scan with AntiVirus. This will let the tool alter the registry. Then, scan the computer with AntiVirus with current virus definitions. You should be able to clean the file system after completing these steps.

The following is an example command line that can be used to exclude a single drive:

```
>"C:\Documents and Settings\user1\Desktop\FxNetsky.exe"
/EXCLUDE=M:\ /LOG=c:\FxNetsky.txt
```

Alternatively, the command line below will skip the scanning of the file system, but will repair the registry modifications. Run a regular scan of the system with the proper exclusions:

```
>"C:\Documents and Settings\us
```

Notes:

- The greater than symbol (>) is not part of the path.

- The name of the log file can be whatever you select. The name listed is for the sole purpose of this example.

Note: You must have administrative rights to run this tool on Windows NT 4.0, Windows 2000, or Windows XP.

WARNING: For network administrators. If you are running MS Exchange 2000 Server, we recommend that you exclude the M drive from the scan by running the tool from a command line with the Exclude switch. Regardless of whether you do this, before running the tool, back up all the data on the M drive. For information on why this is necessary, read the Microsoft Knowledge Base article, "XADM: Calendar Items Disappear from User's Folders" (Article 299046).

The previous information taken from Symantec's corporate website.[9]

The previous steps show that this tool will remove and repair any files associated with the virus. Using one of these tools is a very good idea even if people stay current with virus definitions. There are available switches if executing from a command prompt. Not to worry about that if you are not familiar with using command language. The tools are downloaded with an executable icon as well. One only needs to double click on the icon and the scan will start.

Secure Practices

Try to pick programs that do not have a large number of vulnerabilities. Scott Granneman suggests, "If you know someone using Outlook Express, get them onto something else ASAP, like Mozilla Thunderbird."[4] Mozilla Thunderbird is an email program that can be downloaded from the Mozilla website. Use an anti-virus program and keep your virus software and definition files up to date. Update your operating system regularly with patches. Do not trust any message

or attempt to get your information unless you can absolutely verify the source to be authentic. In reality that is almost impossible so if an email is questionable then delete it. If you are confused get help. Find someone who knows and let them help you start practicing secure computing. Research a subject. The more informed we are as users the better chance we have of defending ourselves against viruses and other attacks. Doing nothing is the worst thing we can do.

Government, Corporate America & Individuals

There are many who are trying to fight this fight. Because of the seriousness of threats that viruses like MyDoom and other types of cyber crimes pose the United States government is even trying to help.

> In a recent article found in the E-Commerce Times Elizabeth Millard states, "Beyond reaching out to the technology industry, the government also has tried to appeal to private citizens to be more vigilant about Internet security. Last March, soon after President Bush issued the ultimatum to Saddam Hussein to leave Iraq or face military action, the Department of Homeland Security asked U.S. residents to report any suspicious cybersecurity incidents or intrusions as part of a nationwide action plan code-named Operation Liberty Shield."[5]

The Department of Homeland Security also has plans for alerting system that will help businesses and individuals report security issues according to the article. A number of large Security software vendors recently sponsored an effort to help educate consumers. Personal Firewall Day was designed to educate the average PC user and give professional security people a chance to share their knowledge with others to sponsor secure computing. The website for this group sponsored event is listed in the resource section of this paper. Another recent article shows some of the efforts also made by state governments. A California law intended to combat I.D. theft took effect July 1st, and obligates companies doing business online to warn their California customers in "the most expedient time possible" about any cyber security breach that exposes customers' names in association with their social security number, drivers license number, or a credit card or bank account number.[6] Chances are that the Internet Service Provider (ISP) we use to provide our connectivity does more than we will ever see. ISP's like other companies have anti-virus software running at large connecting points known as gateways. Fortunately that is another layer of protection but obviously this does not catch everything. The software vendors who write anti-virus software many times publish free fix tools for people who are not running anti-virus software. Microsoft is making efforts to write software patches for vulnerabilities in their operating systems. They are also spending billions of dollars to integrate security into future operating systems and software. There are many who are trying to fight the battle against computer viruses but maybe the most important piece of the puzzle in the are the individuals like you and I that are sitting at their computer right now writing papers or browsing the web. We have to take actions ourselves to make a more secure computing

environment. I consider it my duty to protect my own information and also believe that it is my responsibility to keep my computer from being used by others in attacks against corporations or governments. I hope that you too will take this information and act on it.

IV. Conclusion

Have you ever missed work because of a virus? Influenza affects millions of people each year impacting a person's productivity. Likewise computer viruses cause significant productivity issues for corporations and individuals. The recent myDoom virus is an excellent example of this. This particular virus was a worm with a very good propagation method. The virus effectively spread to hundreds of thousands of computers using up network bandwidth which impacted many corporation production networks. The code was written to later execute a Distributed Denial of Service (DDOS) attack against SCO a computer software company. On the programmed date thousands of computers literally took SCO's website out of business. Computer viruses are a serious threat to all of us. Most are written to take advantage to some type of security hole or vulnerability. Some are written to take advantage of the user as well. In order to protect yourself or business it is necessary to take action. The first thing that needs to be done is find a reliable anti-virus solution, implement and maintain it. Use common sense and make sure you validate everything that looks suspicious. If you are unlucky enough to be infected solicit help or use a fix tool provided by Anti-virus software vendors. Finally keep yourself informed. The more you know about potential security risks the easier it is to find solutions. McAffee and other vendors offer many resources including virus glossaries.

V. Where do I find more help? Resource list

Anti-virus software is only one way to protect yourself from computer viruses. It is very important but there are other places to find help if you are still confused. If my explanations and information have not been helpful enough try doing some research of your own. If you are beginner then start slow. This stuff can be overwhelming. Get some help from the professionals if necessary. The following websites and books are great resources in your quest to keep out the bad guys. Good luck!

Books

Network Security for Dummies by Chey Cobb
The Personal Internet Security Guidebook: Keeping Hackers and Crackers out of Your Home by Tim Speed
Computer Security for the Home and Small Business by Thomas Greene
Home Security: All Thumbs Guide by Robert W. Wood
Safe & Secure: Secure Your Home Network, and Protect Your Privacy Online by Arman Danesh, Felix Wai-Yin Lau, Ali Mehrassa

Websites

Anti-virus software

http://www.symantec.com
http://us.mcafee.com
http://www.sophos.com
http://www.trendmicro.com
http://www.pandasoftware.com
http://www.my-etrust.com

Personal Firewall

http://www.f-secure.com
http://www.firewallguide.com
http://www.zonelabs.com
http://www.sygate.com
http://www.tinysoftware.com

Security Infomation

http://infosecuritymag.techtarget.com
http://www.securityfocus.com
http://www.cert.org
http://www.personalfirewallday.org
http://www.microsoft.com

Other

http://www.microsoft.com
http://www.mozilla.org/products/thunderbird/
http://www.howstuffworks.com
http://www.ask.com

1. Brain, Marshall. "How computer viruses work." Howstuffworks. URL: http://computer.howstuffworks.com/virus.htm (December 31, 2003).

2. UK Security Online Ltd. "What is a computer virus?" UK Security Online. URL: http://www.uksecurityonline.com/threat/virses.php (March 7, 2004)

3. Kotadia, Munir. "Trojan horse found responsible for child porn." August 4, 2003. URL: http://www.zdnet.com.au/techcentre/antivirus/news/story/0,2000044973,20276799,00.htm (December 31, 2003).

4. Granneman, Scott. "Joe Average User Is In Trouble." October 22, 2003. URL: http://www.securityfocus.com/columnists/193 (December 31, 2003).

5. Millard, Elizabeth. "U.S. Government Plans Cyberalert System." E-Commerce Times. January 28, 2004. URL: http://www.ecommercetimes.com/perl/story/32705.html

6. Poulsen, Kevin. "Online fraud, I.D. theft soars." Security Focus News. January 23, 2004. URL: http://www.securityfocus.com/news/7897 (January 28, 2004).

7. Martin, Kelly. "Worms Hit Home." Security Focus Columnists. January 26, 2004. URL: http://www.securityfocus.com/columnists/216 (January 28, 2004).

8. Houghton Mifflin Company. Webster's II New College Dictionary. Copyright 2001.

9. Symantec. "W32.Netsky@mm Removal Tool." March 08, 2004. http://securityresponse1.symantec.com/sarc/sarc.nsf/html/w32.netsky@mm.removal.tool.html (March 15, 2004).