Global Information Assurance Certification Paper

EDUCATING THE PUBLIC

10 ways to take the fun out of spreading Trojans, viruses, & worms

By Deborah Hamdani

March 2004

GSEC Practical Assignment v1.4b, Option 1

Table of Contents

Abstract

This paper discusses educating the public on computer security and 10 ways they can prevent the successful penetration and proliferation of Trojans, Viruses and Worms. The typical home user purchases their computer through some OEM with little to no idea what to do with it once it is set up, other than to email their family and friends, scan and save photos and/or surf the Internet. This typical user may have heard some buzz words about “security”, “viruses”, “worms”, “Trojans” and maybe even “Patches” simply by watching the nightly news. But most have no idea how that affects them or even where to begin with regards to their own computers. The malicious code writers of the world count on this community and their lack of knowledge to spread their “creations”. This paper’s goal is to discuss the 10 things the general computer user should know to protect themselves and their systems from these attacks and to simply take the fun out of writing malicious code.

Introduction

According to the August 2000 US census, 51% of American households had one or more computers. Of that percentage, 41.5% had some form of Internet access, such as dial-up and high-speed. The typical computer user consisted of all family members including children and young adults. The most common Internet usage within the household was sending and receiving email and informational searches. (www.census.gov/prod/2001pubs/p23-207.pdf)

Jump ahead to 2003. The average personal computer cost less than $1000 to purchase and broadband Internet access was available in more places than ever before. The total number of computer owners and Internet users dramatically increased since the 2000 census. Is it a coincidence than that in 2003, Symantec's anti-virus division documented a total of 2,696 new Win32 based Trojans, viruses and worms? Or that there were 5,996 attacks per 100,000 Internet users in the US alone and 2,636 reported new software vulnerabilities, 70% of which were classified as easy exploits? With the most common computer operating system being Microsoft Windows coupled with a large casual computer user population, last year unequalled any other for the amount of successful attacks to computer security. Identity theft has become one of the most common and destructive non-violent crimes committed. And spam has become the biggest money maker for the not so honest, not to mention the biggest headache for email users. All this due to a widespread problem: ignorant computer users getting online for the first time, unaware of the dangers that lurk just on the other side of their modem or broadband router.
(enterprisesecurity.symantec.com/content/displaypdf.cfm?SSL=yes&PDFID=665)

Identity theft and spam are just two of the many consequences if you get infected by malicious code. The common computer user, who on average knows only the basics of computing such as writing and sending email and surfing the Internet, has little idea how Trojans, viruses and worms are even related to these very publicized problems. These types of users are the main target for malicious code writers trying to easily propagate their creations. With so many victims to exploit, it's as if you've left a kid alone in a candy store.

So the question is: Who are these code writers and what drives them? Various studies show that the majority of writers range between the ages of 16 and 26 years old. Most are young adults just looking for a technical challenge while others consider virus writing an art form, or freedom of expression. Some seek to make a political statement. It has become popular for these talented teens and young adults to join or form Internet gangs, communities where to prove ones self you must write a successful Trojan, virus, or worm. Then there are others who have made the choice of joining a new wave of organized crime, writing malicious code to gain financial data through identity theft or for creating viruses that promote the spread of spam. It seems for this age group, malicious code writing has become the newest form of entertainment. Better than video games, hanging out at the mall with friends or watching movies.
(news.bbc.co.uk/1/hi/technology/3172967.stm)

So what can the common computer user do to help stop these malicious code writers? The answer is simple: **Education**. The following are ten items that, if learned and practiced by the common user, will take the fun out of writing malicious code.

Computers 101

Step #1: How does malicious code work?

Before you can define a Trojan, virus or worm, you must understand how malicious code works. Starting from the basics you have a computer system with many **programs** installed on it, including an operating system, an Internet Web Browser and possibly an email application. Each of these programs is made up of individual (and sometimes shared) **instructions** that are performed in a specified order. When operating systems such as Windows first came out, these instructions were written with no thoughts for security. The more educated people became about computer programming, the more interested they became in what programs out there looked like at the instruction or **code** level. Once the code had been traced through, it became clear how easy it was and still is today to write your own instructions and include them or embed them into these very popular programs. Thus the birth of malicious code writers and the term "vulnerability" as it refers to program code.

A **vulnerability** is a weakness in the structure or logic of the code. To discover a vulnerability one must have access to the code or try reverse engineering the code to see how it works. Some companies exist today solely to find vulnerabilities in software and warn the developer of that product about its findings, so it can be fixed. Others discover vulnerabilities and spread the word through hacker chat rooms and the only way the developer is notified is by the publicity of a new Trojan, virus, or worm. Vulnerabilities can be fixed by the developer and passed on to its customers, if that developer has the right communication policy in place. It is up to the customer to take the prescribed action from the developer to fix the vulnerability. It is a race against time usually between the developer, the consumer, and the malicious code writer. In steps Trojans, viruses and worms.

Step #2: Taking the mystery out of Trojans, viruses and worms by defining each.

The common user may have heard the words Trojan, virus and/or worm used before. Maybe some have seen reports on the news about their destruction or even experienced the disruption one of these can cause in their workplace. But few really understand what they are. And without having this vital knowledge, it's hard to prevent their spread.

Although Trojans, viruses and worms are similar and some use the words interchangeably, there are many differences. A **Trojan** is a destructive program known as Spyware. Trojans received their name based on Homer's Iliad and the story of the battle for Troy. The Greek soldiers offered up a giant wooden horse to the city of Troy as a gift to end the fighting between the two cities. Unbeknownst to the city of Troy, this horse was filled with Greek soldiers waiting for the right moment to attack. Trojans in the computer world work much the same way. They may look like an innocent attachment sent by a friend or may even be embedded in a freeware or shareware program you've knowingly downloaded and installed. But in fact it is waiting for the right moment to take control of your computer, deleting files at will, obtaining data and

sending it back to the creator and even leaving behind programs called backdoors that "spy" on your keystrokes and Internet interests. The one significant action a Trojan cannot perform is not being able to replicate itself. It must be sent on either by an email attachment or through an embedded program.
(http://www.webopedia.com/TERM/T/Trojan_horse.html)

A **virus** is a program or piece of code that copies or embeds itself into legitimate programs already on your computer. From there it runs without your knowledge thereby propagating itself. An example of this would be a macro virus. This virus would embed itself into Microsoft Word and run every time Word was opened. It would cause the program to run abnormally, making the user frustrated and eventually corrupting the programs itself, so that it would not execute at all! The user might think it was just the program acting up, reinstall it and start the process all over again.

A virus has four main parts: An **engine** which allows the code to execute and propagate (usually an already legitimate resident program); A **payload** or what its desired affect may be (writing messages on an infected user's terminal or corrupting files); A **host** or the location where the virus can hide out, like in a program or specific instruction or code; And a **trigger**, the event (like opening a resident program) that starts it running. Unlike Trojans, viruses can replicate but needs assistance or human intervention to spread. (www.nightflight.com/foldoc-bin/foldoc.cgi?virus)

A **worm** is a program or algorithm that can replicate itself over a network by taking advantage of automatic file sending and receiving features found on most computers. This transport method works on most networks, including the World Wide Web (WWW). Worms perform malicious actions such as using up system memory, slowing performance or even stopping tasks and shutting down the infected system. Worms differ from viruses in that they do not need a host or engine to spread. Great examples of worms spreading across the WWW affecting vulnerable machines throughout the world were the Blaster and Welchia worms. These worms took advantage of the RPC service running in Windows machines. Infected machines were forced into cyclical reboots until the machine was patched and the worm removed using various removal tools.

Step #3: What's development have to do with it? How about the PC manufacturers and resellers?

So now that we know how malicious code works and what types are out there, the natural question is "How come these malicious code writers are so successful?" "Do they have some kind of magic eight ball to know what code will work across the board of all computers?" The answer is actually very simple. There is a common component to the spread of this code…The operating system. This is the Windows Conundrum.

Microsoft Windows is the most widely used operating system in the world, especially for the home user. When Windows was first released, little to no security was built in. Over the years, as a reactive measure, Microsoft started publishing fixes and new versions of the operating system to stem the outbreak of Trojans, viruses and worms. But the home user typically isn't informed of these new publishes. And most users go by the adage that "if it's not broke, don't fix it" attitude when it comes to their

computers, so they wouldn't be actively looking for these fixes either. They are perfectly content running their legacy Windows computer that might be full of security bugs, because it seems to be working just fine. Of course there is the financial aspect as well. Some home PC owners simply can't afford to turn around every two or three years and invest in all new computer software and hardware. So what can be done?

One idea is to make the developer accountable for their own software. Instead of putting the responsibility on the inexperienced home user, companies such as Microsoft could be more vigilant about following the Software Development Life-Cycle (SDLC). Step number five in the SDLC is simply testing their products before going to market. It appears some Windows flaws could have easily been contained if some basic testing had been put into place prior to going to market. Step number six in the SDLC is product maintenance. Developers should be held responsible for fixing their products, as well as communicating these flaws and getting the fixes to their customers.

Currently Microsoft has a system where you can visit an update website, and software from this site will scan your computer for updates. You then have the option of installing these updates. Although this is a step in the right direction, it is still relying on the home user to have enough awareness to go to the site and look for updates. And this is hardly a respectable solution for those who still live in an area where only dial-up connections are available. It can take many hours just to apply a couple of updates, certainly not incentive to keep your system updated.

One of the biggest changes consumers are pushing for is changes in the software liability laws. Currently developers can hide behind the infamous End-User Licensing Agreements (EULA's) that appear before you can install any software. Most of these agreements have some legalese that releases them from any liability if damage occurs. Simply put, it is an AS-IS warning to the consumer. Use at your own risk. Proponents for the change in software liability laws argue that developers have a "duty of care", meaning that they should be employing simple measures such as testing and maintenance to prevent harm to their customers. They also argue that because consumers are limited in their OS choices, they should not be trapped into purchasing an unsafe product. This is unacceptable in the physical product world (such as with motor vehicles or machinery) and should be equally unacceptable in the software or intellectual world.
(http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2813470,00.html)

To avoid such lengthy legal battles, Microsoft has tried to appease their customers by implementing its Trustworthy Computing Initiative. In January 2002, Bill Gates, founder of Microsoft, sent an email to all of its employees outlining a four "pillar" solution to tighten up their overall software production. He stated that Trustworthy Computing was to take highest priority, even over implementing new technologies. The company spent millions retraining staff on privacy concerns and secure programming practices, as well as restructuring its organization and implementing new processes to help support this new venture. This is touted as a project that will take over a minimum of ten years to implement and many millions more to continue to support. Microsoft's hopes are to create more secure software; build in privacy to help its customers control their confidential data; make their products more reliable; and to take more responsibility for their products by involving a new business integrity plan. (http://news.com.com/2100-1001-816880.html)

However, even with these measures starting to take place, it is important for the common user to still be aware that their main weakness is their software developer. That even with people fighting to make developers more responsible for their products, it is ultimately up to them (the user) to ensure their software is safe from vulnerabilities.

So what about the PC manufacturers? How can anyone ensure their systems are safe if they only have a limited choice at the store? This is where the manufacturer and reseller come in. Until recently, PC manufacturers and resellers such as Dell, Gateway and IBM have not provided much choice in the way of operating systems for home PC's. The De Facto standard is some version of Windows. But if these companies are going to take the stance that Windows is the base operating system, they may also want to take some initiative in making sure the PC is as vulnerable-free as possible, out of the box. Some easy ways to do this are to: **1)** visit Microsoft's update site and ensure any software they've pre-installed for the customer (including operating system, Internet browser and office package) is as update to as possible; **2)** Give the customer a choice of anti-virus software tools to choose from; **3)** Check for services known to have vulnerabilities within the operating system and make sure they are not turned on by default; **4)** Offer a choice of personal firewalls that can protect against attacks coming from the Internet; **5)** Give the customer some training classes to sign up for that may educate them on safe computing; **6)** When selling companion components such as wireless routers or broadband modems, educate the customer on what can be done out of the box to make the use of the product more safe.

Developers, PC manufacturers and resellers must remember that a happy customer is one that will return to buy more in the future and they are also the cheapest form of marketing. If you provide a valuable service, the customer will be sure to pass the word along, free of charge.

Taking Action: Using what you have learned

Step #4: Patching your software, not your jeans!

As previously discussed, all software consists of lines of code. This code may contain vulnerabilities. Vulnerabilities are not just Windows problems. All software programs can be affected by vulnerable code. If these vulnerabilities are discovered, the software developer may create a fix called a patch or hotfix. Similar to patching your favorite pair of old jeans so that you can continue wearing them, the developer writes extra code to plug the security hole or cover the vulnerability.

Currently, it is up to the customer to make sure patches and hotfixes are applied. As a responsible pc owner and Internet user you must be aware of which applications are running on your computer, who the accountable vendor is for its maintenance and when and where to look for available patches. This is a big responsibility and can be a time consuming process. Malicious code writers count on the fact that this process is cumbersome and not practiced regularly by the average computer user to propagate their creations. Thus, there is a new movement among the computer security profession to push the developer to include some automation in patch application. An example of this would be Microsoft's Automatic Updates Service in newer versions of Windows. This service, once configured by the user, can automatically go to Microsoft's update

site at specified times of the day, download the necessary fixes and then notify the user that they are ready to be installed. If the right option is chosen, it will even install the fixes automatically with little to no interaction needed by the user. Two draw backs to this are that **1)** the service does not currently come turned on automatically, but instead needs to be configured by the user and **2)** You must obtain the latest version of Microsoft Windows. If you have an older PC, chances are you need to invest a little more money than just some new software in order to take advantage of this service.

Simultaneously, there is another push to make the PC manufacturers and resellers help apply patches, so that systems are more secure out of the box. This in conjunction with offering other security products bundled with a system purchase could help get a new computer and its user more safety aware and secure from the start.

Applying patches to your vulnerable machines is the single most important thing you can do to prevent Trojans, viruses and worms from infecting you. If they are applied as soon as they are released, the proverbial front door is closed on your system with a posted sign saying "Do Not Enter". What fun is it to create malicious code for vulnerabilities that have already been fixed on your system?

Step #5: Installing Antivirus Scanners

While you are patching your system you might as well install one of the many popular virus scanning software packages. Virus scanners are unique because they are both proactive and reactive. They are typically always on, scanning for the latest malicious code. Antivirus software comes in many forms. Some scan hard drives and other media for a known list of malicious code signatures, while others can prevent code from being executed. Still others can even fix systems that have become infected. The common element in all these variations is that the software must also be updated, typically on a daily basis, just to stay on top of all the rampant malicious code out there. These updates are called definitions or DAT files. The files function much like a "beat cop", walking around your system holding a picture of known malicious code or signature of code, asking if its been seen in the neighborhood. But it needs constant updating because the signatures or pictures of malicious code are constantly evolving and changing their look, much like criminals do to avoid being recognized and arrested. Similar to current operating systems, most of these programs now have automation built in to assist in updating these definition files. But just like the operating system, the draw back to this automation is that it needs to be configured by the user as to the criteria of downloading the updates. Typically there is a wizard that can help walk you through setting up a schedule that best fits the users' needs and connection type.

Anti-virus programs are especially useful if your email is full of attachments forwarded on by friends or if you enjoy downloading freeware or shareware from the many download sites on the Internet. Most antivirus software can scan your emails as they are being delivered to your inbox for any infected or malicious attachments with known signatures. Many scan files being asked to execute whether you are double-clicking on an attachment or double-clicking on an executable file for a program you have downloaded.
(www.solutionsreview.com/antivirus_how_do_antivirus_software_work.asp)

By adding anti-virus to your consistently patched system, you are also adding an advanced monitored alarm system to the already closed front door with a posted warning. What fun is it to write code for a system that has not one but two road blocks in the codes way?

Step #6: Border Patrol: Stopping the burn with a Personal Firewall

Like virus scanners, there are Internet traffic scanners called firewalls. They come in two forms, either hardware or software. For the home user, it typically comes in the form of software, called a personal firewall. The term firewall was adopted from the construction industry because of its similar function. In construction a firewall is built as a sturdy wall, usually made from brick, covering an area from ground to roof in hopes of preventing a fire from spreading in a housing or business community.

In the computer world a firewall is setup to block unauthorized traffic ("the fire") from entering a computer or network from another computer or network, such as the World Wide Web. Firewalls work similar to anti-virus scanners in that it is always on, waiting and watching. It watches for any communications either inbound or outbound that has been deemed unauthorized by its owner or administrator. A good association would be border patrol. At major country borders, such as between the US and Mexico you have a road block or wall that separates the two countries. There are booths with guards stationed on either side controlling the flow of traffic leaving and entering either country. Typically you show some form of identification and state your business with that country and based on certain preset protocols, the guards decide whether to let you pass or not. When setting your computer up on the Internet, personal firewalls are considered your first line of defense against malicious code writers and other hacker types, more or less border patrol between your PC and the Internet. This is especially important if you have the type of connection that is always connected online as is the case with broadband and other high speed connections. (http://www.dmccormick.pwp.blueyonder.co.uk/coursecontent/09/9_04a.htm)

Firewalls work especially well with Trojans and worms because they use what are called communication ports, similar to telephone numbers to pass from one computer to another. Software meant to be used among multiple machines will use the common port numbers to call another computer. Firewalls are designed so that you can tell it which ports you want left open for legitimate communications and which ports to close. This gets a little complicated because there are approximately 65,000 plus ports. There are many sources online that can help you figure out which ports should remain open and which ports should remain closed. Some more advanced firewalls already have predefined rules for certain ports, just as with virus software knowing which signatures of code to look out for.

Because there are many choices for these types of products available, it is important to choose wisely. Check with your local computer reseller or online with trusted computing sites to find which products have been evaluated and might serve your needs the best.

By adding a personal firewall to your computer, not only are you closing the door with a sign out front and employing an advanced alarm system, you are also posting an

armed guard out front that all visitors must pass through. What fun is it to try and write malicious code that has all three of these road blocks to penetrate?

Step #7: ILOVEYOU: Knowing your email

The easiest way for a malicious code writer to propagate their creation is by using a little ingenuity and social engineering. The "ILOVEYOU" virus affected millions of email users across the world. It was a simple email where the subject line said ILOVEYOU and a one sentence body asking you to read the attached file, aptly named "Love letter for you.txt.vbs". Many inexperienced computer users saw the tempting email (which appeared to have been sent by someone they knew) and decided to open the attachment. Unleashed was a virus that not only deleted files such as mp3's and jpg's from the users' system but it replicated itself by copying out email addresses from a stored address list. It created new emails to these addresses, attached a new copy of the virus and sent it on its way, making it appear as though it were legitimately sent from the infected sender. This process increased the chances it would be opened by others.

There was another email that was forwarded around for a year or more claiming that everyone had been infected with a new virus that was undetected by any virus scanner. It walked the reader through where to find the file and told them to delete it. The convincing part was that it stated this virus was discover by Microsoft and threw in some other big company names such as AOL and CNN. Unfortunately this email was a hoax and actually caused people to delete a legitimate Windows file.

This is where knowing your email comes into play. When checking your email there are a few rules you can follow that can help you eliminate these messages. **1)** First thing you can do is scan the list of new emails to verify who the emails are from. You can get rid of half of the email in your inbox just by verifying that the sender is unrecognized by you. **2)** Check out the subject line and think..."Would so-and-so send me an email that said ILOVEYOU?" or whatever the subject line may be. Also, combined with #1, you may be able to deduce that the email is spam, delete it and move on. **3)** Look for attachments to the email. Typically an average user would not attach anything more complicated than a picture file (jpg, gif, tiff, bmp etc), word-processing document (doc, wpd, wps etc) or Adobe document (pdf). If the attachment has an extension that you don't easily recognize, don't open it. This would have saved many of the ILOVEYOU victims. **4)** If the email doesn't have an attachment but has a link to a website, be aware that many of these hyperlinks, although look harmless, may bring you to a pornographic website or some type of malicious code waiting to be downloaded on your computer. If you have your virus scanner running and your personal firewall scanning communications properly, you should be safe, but imagine if you didn't?! **5)** Finally, use common sense. If an email comes from a vendor you do business with (such as a bank) and has a seemingly legitimate subject line with no suspicious attachments, read the body very carefully. Many new scams nicknamed "Phishing" expeditions try and trick you into following a link to a website where they ask you to enter personal data such as your bank account number etc. The common sense lesson here is, if your bank is emailing you, why would they ask you for your bank account number? Couldn't they just look it up in their own system?! When in doubt, call first and check it out before following along.

Keeping up with the malicious code writing Jones'

Step #8: Being Proactive

On top of installing patches, antivirus software, personal firewalls and maintaining a handle on your email there are several other things you can do to avoid being the recipient of malicious code. **1)** Scanning removable media for viruses. Floppy disks, cd's, and USB memory sticks are handy for transporting data from one place to another, but they are also a handy way to transport malicious code. Most anti-virus software has built-in tools allowing you to check these devices before attempting to open any of their content. **2)** Spyware scanning. Spyware is executable code installed typically without the user's consent and is designed to obtain personal data and use it for either marketing purposes or more malevolent activity such as stealing your identity. Examples of spyware include Trojans, System monitors, Dialers, Adware and Adware Cookies. Spyware will eat up system resources and Internet bandwidth. Without specialized scanning software it can be next to impossible to detect and remove these types of spyware. Some anti-virus programs also search for spyware, but there are also inexpensive products on the market to help keep your system clean of these threats. (www.webroot.com/wb/products/spysweeper/spywaredefined.php) **3)** Keeping Internet cache clean and removing cookies. When you enter a website, certain information including links and some pictures are stored on your computer. Originally the intent of this locally stored data was to make for quicker downloads of that site if returned to at a later date. However, deceitful website owners may design their cookies to collect valuable personal data about you and store it in "Cookies" on your computer without your knowledge. These cookies are left on your machine after you have visited certain websites, taking up space on your hard drive, but more importantly, allowing other marketers to access the data. These marketers can gather personal information about you including buying habits and surfing habits. Most web browsers have a way of helping you clean out your Internet cache and cookies, but some spyware removers will also help. It is important to remove this information on a routine basis. **4)** Checking the logs of your antivirus and personal firewall software. It is important for you to be aware what your scanning engines are finding. Staying informed about what types of attacks are entering your system will help you fine tune a plan that works best for your type of computer use. Turning on logging from your operating system is also a good idea if your system supports it. Most operating systems allow you to track who is logging onto (or attempting to log on to) your system, which programs and resources are being accessed (by date, time and user) and even when your system has been shutdown or rebooted last. These things can tell you if you have undetected spyware or other malicious code running on your computer. **5)** Controlling services – knowing which ones to turn off and ones to keep on. In later versions of operating systems such as Microsoft Windows, users have the ability to turn certain services or programs that run in the background on or off. Some of these services actually contribute to the vulnerabilities the virus writing Jones' are trying to keep up with. Unfortunately it has been common practice by the vendor to have all these services turned on out of the

box. By knowing which services might pose a threat to your system and by disabling them, you are staying one step ahead.

Step #9: This just in: Public Alert systems

In January, after a break out of a virus called MyDoom, the Department of Homeland Security (DHS) decided it was in the best interest of our nation's computer infrastructure if they created an alert system. Its intent is to help give out early warnings to government agencies, businesses and home users about new security threats and how to mitigate those threats. They are also devising a system involving email to help educate home users on how to better secure their computers. Users can sign up for security email bulletins from the DHS by going to www.us-cert.gov. This division of the DHS is headed by a former executive at Symantec Corporation, an anti-virus and computer security software developer. Signing up for bulletins such as this one, provided free of charge can help keep the casual user informed about their systems vulnerabilities.
(http://www.computerworld.com/securitytopics/security/story/0,10801,89488,00.html)

Simply watching the nightly news can also help you stay on top of your systems vulnerabilities. Many news agencies now report outbreaks of major viruses including pertinent details such as if it is sent by email, what the subject line may be and what to do if infected. By staying informed through one of the avenues, you can keep your system to becoming one of the infected systems, staying one step ahead of those malicious code writers.

What if I've just skipped to this last page?

Step #10: What to do if you become infected

If you have skipped through this document and do get infected with some type of malicious code, all is not lost. Here are some things you can try: **1)** Do not panic. Disconnect your computer from the Internet, especially if you have a persistent internet connection such as always on broadband. The last thing you want to do is contribute to the spread of the code. **2)** Try and identify what it is you are infected with. You can do so by visiting any one of the major antivirus companies' websites. They usually have the latest list of viruses out there with links on how you can get rid of them. However, these solutions usually cost money, so keep an open mind about spending some green to resolve your problem. **3)** Visit one of your software vendors' websites. If the malicious code is attacking a vulnerability in their product, typically a patch and instructions for removing the offending code will available for download. **4)** Warn people you frequently email or otherwise exchange electronic data. This will ensure to minimize the impact of an unintentional spread. If you know what you have been infected with and have some knowledge of its removal process, share that information as well. **5)** Obtain a license for anti-virus software, a personal firewall and possibly spyware scanning software as well. Be sure your system is up to date with all its patches and sign yourself up for a free bulletin on how to keep your system free from infection.

Conclusion

The best way to take the fun out of writing malicious code is to educate yourself on how software works; how vulnerabilities play a part in the security of your system; stay informed on what to do about the vulnerabilities affecting your system; and how to be proactive without spending a lot of time worrying about security. Use common sense when using your systems such as email. Be careful what you download off the Internet and what sites you visit. If there are no vulnerable systems to exploit and no gullible email users to trick into opening the wrong attachment, then the potential of successful propagation of malicious code is minimize. Where's the fun in that?

Bibliography

Berlind, David. "Is Microsoft liable?" September 19, 2001. URL: http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2813470,00.html

"Firewalls: What is a firewall?" URL: http://www.dmccormick.pwp.blueyonder.co.uk/coursecontent/09/9_04a.htm

"How does Antivirus Work?" Updated 2003. URL: www.solutionsreview.com/antivirus_how_do_antivirus_software_work.asp

Homepage. URL: www.us-cert.gov

Lemos, Robert and Kane, Margaret. "Gates: Security is top priority". January 17, 2002. URL: http://news.com.com/2100-1001-816880.html

Newburger, Eric. "Home Computers and Internet Use in the United States: August 2000", p.1 URL: www.census.gov/prod/2001pubs/p23-207.pdf

"Spyware defined". Updated 2004. URL: www.webroot.com/wb/products/spysweeper/spywaredefined.php

"Symantec Internet Security Threat Report: Volume V" p. 4, 7, 11. URL: enterprisesecurity.symantec.com/content/displaypdf.cfm?SSL=yes&PDFID=665

"Trojan Horse". URL: http://www.webopedia.com/TERM/T/Trojan_horse.html

Twist, Jo. "Why people write computer viruses". August 23, 2003. URL: news.bbc.co.uk/1/hi/technology/3172967.stm

Verton, Dan. "DHS launches national cyber alert system", January 28, 2004. URL: http://www.computerworld.com/securitytopics/security/story/0,10801,89488,00.html

"Virus". Updated December 3, 2000. URL: www.nightflight.com/foldoc-bin/foldoc.cgi?virus

Last Updated: September 19th, 2017

Upcoming Training

Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS New York SEC401*	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Mentor Session - SEC401	Minneapolis, MN	Oct 03, 2017 - Nov 14, 2017	Mentor
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VA	Oct 14, 2017 - Oct 21, 2017	Live Event
SANS Tokyo Autumn 2017	Tokyo, Japan	Oct 16, 2017 - Oct 28, 2017	Live Event
CCB Private SEC401 Oct 17	Brussels, Belgium	Oct 16, 2017 - Oct 21, 2017	
Community SANS Omaha SEC401	Omaha, NE	Oct 23, 2017 - Oct 28, 2017	Community SANS
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201710,	Oct 23, 2017 - Nov 29, 2017	vLive
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
Community SANS Vancouver SEC401*	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
Community SANS Colorado Springs SEC401**	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event