Interested in learning more about security?

SANS Institute
InfoSec Reading Room

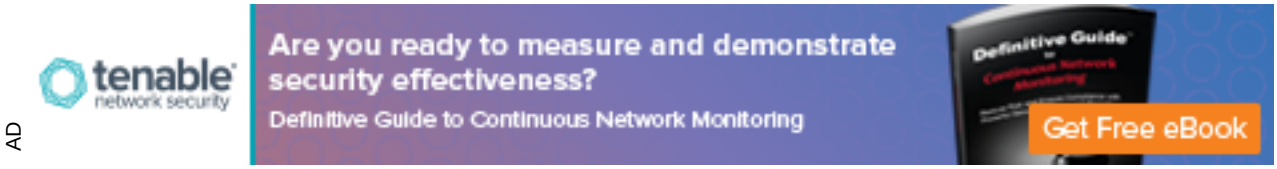
This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Home User's PC Security: Threats To Windows Users and Countermeasures To Defend Against These Threats

The objective of this paper is to alert home users of the growing number of threats to home PCs and to provide proper countermeasures against these threats. Eventually, the ultimate goal is to minimize security incidents attributed to these threats with proper countermeasures.

Copyright SANS Institute
Author Retains Full Rights

AD



Home User's PC Security: Threats To Windows Users and Countermeasures To Defend Against These Threats

Table of Contents

1.0) Objective
2.0) Target Audience
3.0) Problem Statement
4.0) Overview
5.0) Security Risks to Home Users
6.0) What are the threats?
  6.1 Broadband Internet Connection: DSL and Cable Modem
  6.2 Malicious codes/programs and backdoors
  6.3 Denial of service (DOS)
  6.4 Distributed denial of service (DDOS) agent
  6.5 Email spoofing
  6.6 Worms transmitted via email attachments
  6.7 Unsecured Windows file shares
  6.8 Cross site scripting
  6.9 Active content in Java/Java Script/ActiveX
  6.10 Packet sniffing
  6.11 IRC clients
  6.12 Hidden file extension
7.0) What are the counter measures to these threats?
  7.1 Secure DSL connection
  7.2 Patch systems with latest patches
  7.3 Install personal firewalls
  7.4 Install anti-virus softwares and malicious program detectors
  7.5 Safe email practices
  7.6 Do not open unknown programs
  7.7 Disable hidden file extensions
  7.8 Protect file sharing.
  7.9 Disable Java/JavaScript/ActiveX
  7.10 Disable scripting features in email programs
  7.11 Make regular backups
  7.12 Always keep an emergency boot disk.
8.0) Conclusion
9.0) References

© SANS Institute 2001, Author retains full rights

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

1.0 Objective

The objective of this paper is to alert home users of the growing number of threats to home PCs and to provide proper countermeasures against these threats. Eventually, the ultimate goal is to minimize security incidents attributed to these threats with proper countermeasures.

2.0 Target audience

This paper is focused to address home users using Windows operating system, i.e. Windows 95 and Windows 98. Based on my studies and comparisons of the different operating systems used by home users, many security incidents, such as worms transmitted via emails, flaws in file sharing affect home PCs running on Windows operating system compared to any other operating systems. CERT Advisory CA-2001-20 has reported of over 23 000 machines had been infected with the W32/Leaves worm, discovered in July 2001, which targets home users running on Windows operating system.

3.0 Problem Statement

The problem statement of this paper is that home users' PCs running on windows operating system pose many threats. Therefore, this paper will recommend proper solutions to countermeasure these threats.

4.0 Overview

The current situation shows many home PCs have become victims of virus and worm infections, DDOS agents and many others as discussed in the paper. Based on my observation, the increasing number of worms transmitted via emails affecting home users are as a result of unawareness of the threat and improper countermeasures such as safe handling of email attachments and not keeping an updated anti-virus in their PCs. CERT Incident IN-2001-07 has reported of a new worm targeting home users running on Windows operating system, W32/Leaves worm, discovered in July 2001 and CERT Advisory CA-2001-20 has reported of over 23 000 machines had been infected with this worm.

The above incident reveals there still lies a gap, between the ultimate defense needed for security and the existing defense in practise among home users. This gap needs to be rectified with proper countermeasures and defense mechanisms.

Lemos Robert in his article in ZDNet News (February 16, 2000) at http://www.zdnet.com/zdnn/stories/news/0,4586,2439985,00.html
has quoted Eugene Spafford, a computer science professor and security expert from Purdue University that home users don't have the right security tools and understanding about why they need them and they are much more likely to be prone to attack or their machines used in DDOS, coordinated attacks.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

5.0 Security Risks to Home Users

Information security is concerned with three main areas;

a) Confidentiality -information should only be available to those authorized to have access to it),
b) Integrity -information should only be modified by those authorized to do so
c) Availability -information should be accessible to those who need it when they need it

Security risks to home users are attributed to confidentiality, integrity and availability. Unauthorized access to financial records, credit card number and password risk the confidentiality of information stored plainly in PCs. The integrity of the information is at risk when an attacker alters and modifies the data in your important documents. The availability of a home user's information is at risk when an information can be erased or become inaccessible as a result of denial of service.

6.0 What are the threats?

In this section we will identify and understand what are the threats to home users PCs and the consequences or incidents associated to these threats.

6.1 Broadband Internet Connection: DSL and Cable Modem

Broadband technology such as DSL and cable modem connection has contributed to the growing number of home PC threats. This threat affects users of other operating systems as well. The 'always on' and no 'connection setup' waiting features which are much preferred by users actually make this kind of connection more susceptible to attacks. Though, a user has closed the browser and works on other applications, somehow the connection is still on and is visible to outsiders.
The risk of an unsecured DSL connection is an unauthorized access from the Internet to a host on the local network (on the LAN side of the DSL router/modem).
The "shared-medium" topology of a cable modem is more susceptible to risks such as packet sniffing and unprotected windows sharing than DSL connection but many of the other threats to home users PC apply to both DSL and cable modem access. However, this does not mean dial up connection is totally secured and does not pose any threats.

6.2 Malicious Codes/programs and backdoors. Malicious codes and programs refer to virus (that reproduces by attaching to another program), worm (an independent program that reproduces by copying itself from one system to another, usually over a network) and trojan programs (an independent program that appears to perform a useful function but that hides another unauthorized program inside it). CERT Incident IN-2001-07 has reported a new worm, W32/Leaves worm discovered on July 2001, which targets home users. It has a functionality which allows an attacker to modify the behavior of the worm

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

infected on a machine and permits an attacker to control the compromised machine's network. Malicious code can cause significant security breaches such as jeopardize the availability of information once it infects programs/files and corrupts them thus making them inaccessible. A trojan program installed successfully in your PC, can permit an intruder to access or modify any information available in the PC and worst still the software configuration of a computer can be changed to permit subsequent intrusions.

A backdoor or a remote administration program once installed successfully in a PC, gives an attacker root access to the whole system. The implication of backdoor can risk the confidentiality of the information. An intruder can access or steal sensitive information from the victim computers, i.e. username/password, credit card number. Common tools used to get a backdoor access are Netbus, BackOrifce and Subseven.

6.3 Denial of service (DOS): Home users should be cautious that they are as much likely vulnerable to DOS attacks just like any other organizations. DOS ranges from flooding a network to disrupting connections between two legitimate machines. This attack could essentially disable your computer and slow down the performance thus affecting the stability of your computer. A major risk caused by DOS attack is the loss of availability to information, when information becomes inaccessible to an authorized user.

6.4 Distributed Denial of Service (DDOS) Agent. Lately, home users' PCs have become targets for DDOS agents. Recent reports by CERT Advisory CA-2001-20 reveals there is an increasing number of compromises on home users' PC which are then used as launching ground for attacking other systems in a distributed denial of service. In a distributed denial of service, a few compromised PCs are used as DDOS agent by using trojan programs and they are instructed by a single “handler” to launch denial of service. Thus your computer is just a convenient tool or a contributor in a larger attack. A new DOS program, the Tribe Flood Network is installed in compromised computers weeks or months before the attack. Another DDOS tool known as "Knight" was found on approximately 1500 hosts as reported by CERT Advisory CA-2001-20. This tool also uses IRC as the control channel.

6.5 Email spoofing

Home users are also vulnerable to the threat of email spoofing. When someone spoofs your email, it means that he/she is sending a fraud email message making it appears to come from one legal sender when actually it comes from another illegal sender. The main purpose of such malicious act can be to impersonate an actual user into making a damaging statement or revealing confidential information, thus risking the confidentiality of the information. An example is as an email claiming from your ISP requesting your username/password or account information or to change your password.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

6.6 Worms transmitted via email attachments.
Windows users are exposed to the threat of worms and other types of malicious code which are often spread as attachments to e-mail messages, particularly via Microsoft email programs.

An example is the Melissa virus, discovered in April 1999 which spread precisely because it originated from a familiar address. Also, malicious codes can be distributed in amusing or attractive programs. And the recent example is the wide spread of W32SIRCAM worm, discovered in July 2001, which propagates via Microsoft Outlook email programs and comes in various attractive attachments loaded with personal files belonging to the victim and is a temptation to any users to open the attachment.

6.7 Unsecured Windows file sharings.
Anyone with File and Print sharing enabled and using share level access are exposed to this threat, a common source of security problem under Windows operating systems. The flaw in an unsecured windows shares can be exploited by intruders in an automated way to place tools on large numbers of Windows based computers attached to the Internet. An unsecured windows shares together with DOS tools can become a great opportunity for intruders to launch DOS attacks. It was discovered recently that there is a flaw in the way that Windows handles the passwords for file sharing. An attacker still can access a password protected shared driving without knowing the full password just the first character of it. A special program can be easily written to exploit the problem and in fact are already circulating around the Net, to be abused by intruders everywhere.

6.8 Cross Site Scripting. A malicious web developer may attach a script to something you send to a web site. When the web site you are browsing from your home PC responds back to you, the malicious script embedded in it comes along into your browser. Browsing untrusted sites, email messages, or newsgroups postings and using interactive forms on an untrustworthy site can expose your web browser to malicious scripts. By exploiting this codes, the confidentiality of your information is at risk as an attacker can steal your password and other sensitive information. Attackers may also be able to use malicious scripts to infect cookies with copies of themselves. If the infected cookie is sent back to a vulnerable web site and passed back to your browser, the malicious script may start running again.

6.9 Active content in Java/Java Script/ActiveX . Active content or active code is a program code embedded in the contents of a web page. Examples are in Java, JavaScript and ActiveX. The embedded code is automatically downloaded and executed to the user's PC once the page is accessed by a browser. Although the code is basically useful, but it pose dangers where intruders can gather information (such as which web sites you visit) or to run malicious codes on your computer.

6.10 Packet sniffing. A packet sniffer run by an attacker has the capability of capturing every data in information packet on a network and of decoding all seven layers of the

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

OSI protocol model. The data may include user names, passwords, and other confidential information that travels over the network in plain text. Passwords captured by a packet sniffer allows an intruder to gain full control and launch attacks on systems. Cable modem users are more susceptible to packet sniffing than dial up users since entire neighborhoods of cable modem users are effectively part of the same LAN.

6.11 IRC Clients. Internet chat applications, such as MSN instant messaging applications and Internet Relay Chat (IRC) networks enables transmission of information over the network which includes exchange of conversations, web URLs and files including the exchange of executable codes. This pose dangers and risks just like the email clients. Some distributed denial of service tools use IRC as the control channel, such as the tool known as "Knight" discovered by CERT/CC reported in CERT Advisory CA-2001-20.

6.12 Hidden File Extension.
Lately, it was discovered that there are recent malicious programs exploiting the default behavior of Windows operating systems which hides file extensions from the user. This behavior can be used to trick users into executing malicious code by making a file appear to be something it is not. The option is enabled by default, but a user may choose to disable this option in order to have file extensions displayed by Windows. Many worms transmitted via emails are known to exploit hidden file extensions.

An example of a worm exploited the hidden file extension was the VBS/LoveLetter worm, discovered in May 2000 which contained an e-mail attachment named "LOVE-LETTER-FOR-YOU.TXT.vbs". Other malicious programs have since used similar naming schemes. Examples include

VBS/OnTheFly (AnnaKournikova.jpg.vbs) - discovered in February 2001
VBS/Timofonica (TIMOFONICA.TXT.vbs) - discovered in June 2000
VBS/CoolNote (COOL_NOTEPAD_DEMO.TXT.vbs) - discovered in May 2000

Basically, any users might think the file sent via emails as attachments are safe as they appear as safe normal .txt, .mpg, .avi files, when actually the file has malicious script or is executable, i.e .vbs, .exe.

7.0 What are the countermeasures to the these threats?
The countermeasures to these threast involve three elements, people, technology and policy. People will be concerned on the awareness, knowledge and skills as countermeasures, technology will be concerned on tools and programs as countermeasures and policies and Standard Operating Procedures to govern the implementation of the countermeasures.

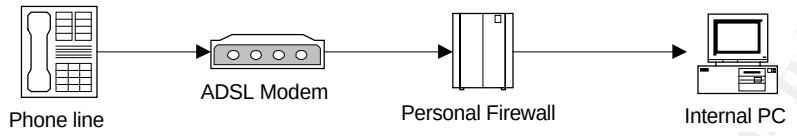
7.1 Secure DSL connection. A secure DSL connections depends on the topology of the component in a DSL connection. The most wide spread use of the DSL format is ADSL which stands for Asymmetric Digital Subscriber Line and is used for residential and small businesses to connect to the Internet at high speeds.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

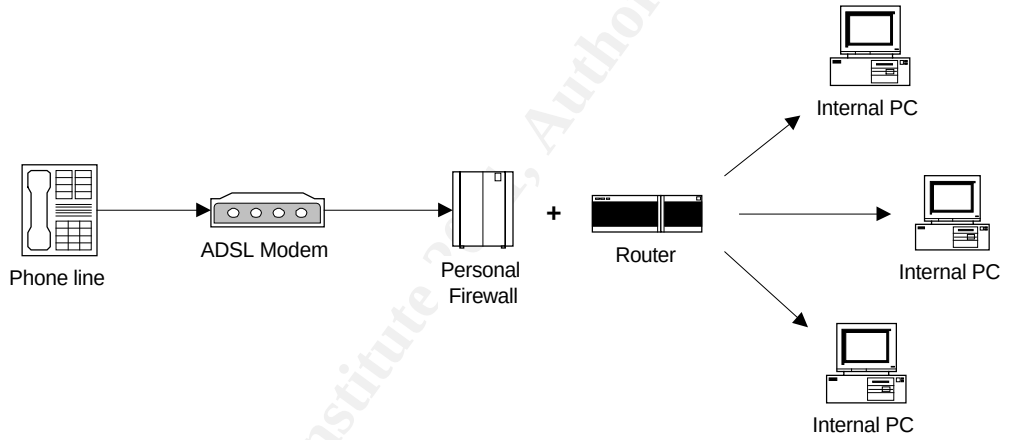
Sean Boran in his article at http://www.securityportal.com/articles/pf-ads120010614.htm has recommended modem topology for a secure ADSL connection. I find this is a good and secure topology for home users using DSL connection.

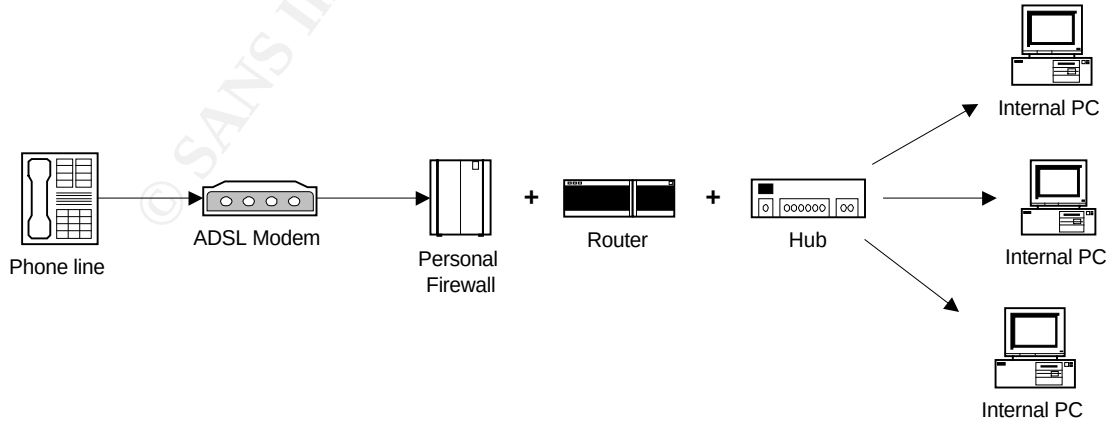
Recommended secure ADSL connection topology:
NOTE: The modem must be external and not an internal card in a PC.

Assuming a single PC is protected:



Assuming a small network of up to a few PCs are protected





© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Generally, another way is to turn off your computer or disconnect its Ethernet interface when you are not using your computer as an intruder cannot attack your computer if it is powered off or otherwise completely disconnected from the network.

7.2 Patch your system with latest patches. I have seen many security incidents attributed to .vbs virus and unprotected file sharing are as a result of not keeping updated with Microsoft's latest patches. Microsoft (http://www.microsoft.com) is always coming up with latest patches to patch any vulnerabilities discovered on Windows operating systems. These patches are critical to defend against vulnerabilities in Windows and Internet Explorer.

7.3 Install a personal firewall. Basically, a personal firewall defends computers and networks from malicious and unauthorized access or connections. Personal firewall alerts users when someone is attempting unauthorized connection to their PCs and has the ability to block intruders from connecting to the computer again.

I have reviewed and found the following personal firewalls as good defense mechanism against these threats.

Zone Alarm has the capability to close netbios port and other ports in Windows operating systems, will stealth ports and stop covert information exchange in the system. It is available at http:// www.zonelabs.com. Zone Alarm's newest version also has a feature to help guard against .vbs viruses. These programs are also good to use for small networks using a dial up connection, DSL or cable modems. ATGuard can be configured to handle ActiveX and JavaScript and restrict access to other areas of your system. BlackIce Defender has the packet-filtering firewall component and intrusion detection component which has stateful inspection capabilities to monitor the system. Interestingly, Black Ice Defender can identify a malicious traffic before permitting the traffic in and upon detection it will alert you, log the activities and block it. Black Ice Defender is also able to gather information about the attacker such as host name and MAC address.

7.4 Install anti-virus softwares and malicious program detectors. It is important to have an updated version of anti-virus softwares installed in your PCs to scan and detect the presence of any virus. They look for patterns in the files or memory of your computer that indicate the possible presence of a known virus. Anti-virus packages know what to look for through the use of virus profiles (sometimes called signatures") provided by the vendor. Anti-virus should be updated with latest virus definitions or the anti-virus should support automatic updates in order to detect new viruses since new viruses are discovered daily. List of well known anti-virus vendors is available at http://www.mycert.org.my/antivirus.htm

A trojan horse detector is also fairly important and most anti-virus softwares can detect trojan horses. Tauscan, a trojan horse detect program, available at http://www.agnitum.com, is updated daily and can detect and remove trojans in

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

computers. Other such programs are Netbus Detective which detects all incoming netbus activities and remove any trojan horses attributed to netbus.

Jammer is a scan detector and registry monitor. It also stops varieties of Back Orifice and Netbus before they can be installed into a system and for any suspicious change detected to the registry (such as the introduction of a trojan) it will ask whether or not to allow the change. If not, Jammer will delete the program.

7.5 Safe Email Practices. A general practise is not to open unknown email attachments. Before opening any e-mail attachments, be sure to know the source of the attachment and if you need to open it, you need to disconnect your computer's network connection, save it to your hard disk and run a virus scan with an updated anti-virus, enabled to scan all files on the attachment. It is not enough that the mail originated from an address you recognize. Be cautious that malicious code can be distributed in amusing programs with attractive subject headings, such as the recent W32 SIRCAM worm, discovered in July 2001 which comes in attractive subjects and is a temptation to any users to open the attachment.

Avoid sending messages with attachments that contain executable codes, like Word documents with macros, EXE files and ZIPPED files. You can use Rich Text Format, or RTF, instead of the standard .DOC format. RTF will keep your formatting, but will not include any macros. There is, however, a couple of viruses out there that will fool Word when you save as RTF, so while you cannot completely trust .RTF files it is still a good practice. This may avoid the embarrassment of you sending them a virus if you are already infected.

In Microsoft Word 97, enable ‘Macro Virus Protection” by choosing:
Tools --- Options --- General and select the appropriate checkbox.

7.6 Do not open unknown programs. Home users are advised not to open any unknown programs unless it is authored by a trusted party. Also, don't send programs of unknown origin to friends or colleagues simply because they are amusing – who knows, they may contain a Trojan horse program.

7.7 Disable hidden filename extensions. Windows operating systems contain an option to "Hide file extensions for known file types". The option is enabled by default, but you can disable this option in order to have file extensions displayed by Windows. After disabling this option, there are still some file extensions that, by default, will continue to remain hidden.

There is a registry value which, if set, will cause Windows to hide certain file extensions regardless of user configuration choices elsewhere in the operating system. The "NeverShowExt" registry value is used to hide the extensions for basic Windows file types. For example, the ".LNK" extension associated with Windows shortcuts remains hidden even after a user has turned off the option to hide extensions.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

7.8 Protect File Sharing. If file sharing is enabled, you need to protect it from unauthorized attacks. Microsoft recommends that anyone with File and Print sharing enabled and using share level access on a Windows 9x or Windows Me system must install patch which is available at Microsoft's site.

7.9 Disabling Java/JavaScript/ActiveX in your web browser. Netscape Navigator and Internet Explorer have options to customize and tighten browser security to disable Java, JavaScript and ActiveX scripting especially when you are browsing unfamiliar or untrusted sites. By doing this, you are defending your PC against threat associated to mobile code .

To disable Java/JavaScript In Nestcape Navigator
go to Edit -- Preferences--Advanced--Disable Java/JavaScript

To disable ActiveX In Internet Explorer
go to View----Internet Options-----choose to disable Active X

In addition, some anti-virus also has protections against Java/JavaScript/ActiveX such as Norton Anti-Virus and McAfee Anti-Virus which offer some level of Java/ActiveX protection.

7.10 Disable scripting features in e-mail programs. Many e-mail programs, such as Microsoft Outlook use the same code as web browsers to display HTML. Thus the vulnerabilities that affect ActiveX, Java, and JavaScript are often applicable to e-mail programs as well. Therefore, users are also advised to disable these features in their e-mail programs.

In addition, users may also benefit by removing Windows Scripting Host from their Windows environment especially to protect against the VBSscript worm. To do this in Windows 9x, go to 'Control Panel' and choose 'Add/Remove Programs'. Click on the 'Windows Setup' tab and double click on 'Accessories'. Scroll down to 'Windows Script Host' and uncheck it and choose 'OK'. It may be necessary to reboot the system.

7.11 Make regular backups. It is important to make regular back ups of important files and data in case your computer is compromised or damaged. A safe practice is to always keep a copy of important files on removable media such as ZIP disks or recordable CD-ROM disks (CD-R or CD-RW disks). Use software backup tools if available, and store the backup disks somewhere away from the computer. From my review, the current Ghost program, version 6.5, provides many useful utilities to help protect valuable PC system. It has a utility that creates bootable diskettes that can include drivers for network cards, CD drives, writeable CD drives, and USB ports. Another important utility is Ghost Explorer that allows you to search files on an image created by Ghost and even extract files from that image. Generally, this is a very cheap and easy way to backup your system.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

7.12 Always keep an emergency boot disk. I have seen some incidents where a home user's PC infected with a boot sector virus and the victim does not have an emergency boot disk for recovery. Thus, it is wise to keep an emergency boot disk in case your computer is damaged such as by virus attacks (commonly boot sector viruses) or hard disk failure. Creating a boot disk on a floppy disk will help when recovering a computer after such an incident. Remember, however, you must create this disk before you have a security incident.

8.0 Conclusion

Home users should realize that their home PCs are no longer secured in the privacy of their homes. Every home user should be aware and concerned of the ever growing number of threats associated to their home PCs. Nevertheless, incidents attributed to these threats can be minimized with proper countermeasures and safe practices by home users themselves. A combination of various countermeasures can achieve the purpose of defense in depth, the ultimate defense for maximum security. Leaving the job to an anti-virus alone is not sufficient, it should be combined with good personal firewalls and safe email practices for defense in depth. Eventually, knowing all the threats and taking proper countermesures can serve the ultimate goal of the objective of this paper which is to minimize security incidents associated to these threats to the lowest level as possible with proper countermeasures and defense mechanism.

9.0 References:

9.1 http://www.mycert.mimos.my/faq-safe_email_practices.htm
9.2 http://www.mycert.mimos.my/network-abuse/dos.htm
9.3 http://www.winplanet.com/winplanet/reports/2497/1
9.4 Miastkowski, Stan. Fortress PC. May 2001. URL: http://www.pcworld.com/features/article/0,aid,44543,00.asp
9.5 Lemos, Robert. Has Your PC been Hijacked. February 16, 2000. URL: http://www.zdnet.com/zdnn/stories/news/0,4586,2439985,00.html
9.6 Born, Sean. “ADSL: Security Risks and Countermeasures. 14 June 2001. URL: http://securityportal.com/articles/pf_adsl20010614.htm
9.7 Baker, Tracy. Potential Threats To Your PC’s Security. February 2001. URL: http://www.smartcomputing.com/editorial/article.asp?article=articles%2F2001%2Fs1202%2F12s02%2F12s02%2Easp&guid=q7z5htn0&searchtype=0&WordList=Potential+threat+to+your+PC%27s+security
9.8 http://www.nai.com
9.9 http://www.symantec.com
9.10 http://www.cert.org/advisories/CA-2001-20.html
9.11 http://www.cert.org/incident_notes/IN-2000-01.html
9.12 Boran, Sean. Personal Firewall/Intruder Detection System: An Analysis of Mini Firewalls for Windows Users. June 14, 2001. URL: http://www.security.com/articles/pf_main2001023.html

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

9.13 NISER/SANS KL Security Essentials Manual 1.1, 1.2
9.14 http://www.cert.org/tech_tips/home_networks.html

© SANS Institute 2001, Author retains full rights

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: October 10th, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Tysons Corner 2015	**Tysons Corner, VAUS**	**Oct 12, 2015 - Oct 17, 2015**	**Live Event**
SANS Gulf Region 2015	**Dubai, AE**	**Oct 17, 2015 - Oct 29, 2015**	**Live Event**
SANS Cyber Defense San Diego 2015	**San Diego, CAUS**	**Oct 19, 2015 - Oct 24, 2015**	**Live Event**
SANS Tokyo Autumn 2015	**Tokyo, JP**	**Oct 19, 2015 - Oct 31, 2015**	**Live Event**
SANS Sydney 2015	**Sydney, AU**	**Nov 09, 2015 - Nov 21, 2015**	**Live Event**
SANS South Florida 2015	**Fort Lauderdale, FLUS**	**Nov 09, 2015 - Nov 14, 2015**	**Live Event**
SANS London 2015	**London, GB**	**Nov 14, 2015 - Nov 23, 2015**	**Live Event**
Pen Test Hackfest Summit & Training	**Alexandria, VAUS**	**Nov 16, 2015 - Nov 23, 2015**	**Live Event**
SANS Hyderabad 2015	**Hyderabad, IN**	**Nov 24, 2015 - Dec 04, 2015**	**Live Event**
SANS Cape Town 2015	**Cape Town, ZA**	**Nov 30, 2015 - Dec 05, 2015**	**Live Event**
SANS San Francisco 2015	**San Francisco, CAUS**	**Nov 30, 2015 - Dec 05, 2015**	**Live Event**
Security Leadership Summit & Training	**Dallas, TXUS**	**Dec 03, 2015 - Dec 10, 2015**	**Live Event**
SANS Cyber Defense Initiative 2015	**Washington, DCUS**	**Dec 12, 2015 - Dec 19, 2015**	**Live Event**
SANS Las Vegas 2016	**Las Vegas, NVUS**	**Jan 09, 2016 - Jan 14, 2016**	**Live Event**
SANS Dubai 2016	**Dubai, AE**	**Jan 09, 2016 - Jan 14, 2016**	**Live Event**
SOS: SANS October Singapore 2015	**OnlineSG**	**Oct 12, 2015 - Oct 24, 2015**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**