Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

Preventing Your Computer From Becoming a Zombie

Jamy Klein
June12, 2001

Introduction

The advent of always on Internet connections has created a large community of users with high bandwidth connections and little to no security. Hackers, crackers and "script kiddies" increasingly target these users. The machines themselves are not usually a target for data theft, but instead are targeted for use as drones in attacks on other systems.

On February 7, 2000, a wave of Distributed Denial of Service (DDoS) attacks hit high profile websites such as Yahoo and Amazon.com taking them offline. Many of the attacks were traced back to compromised machines at universities infected with a zombie agent. A zombie agent is used to remotely control a compromised machine to carry out attacks. A zombie agent, is a Trojan used to control a user's machine without their knowledge.

Compromised computers on various networks carried out a more recent attack against the security web site of Gibson Research Corporation at www.grc.com. The majority of attacks originated on compromised cable modem connected computers on the @home® network. Steve Gibson, the owner of www.grc.com has posted a detailed transcription of the attacks and his communications with the attackers at http://grc.com/dos/grcdos.htm.

A recent study conducted by the University of California, San Diego determined that approximately 4,000 Denial of Service or DoS attacks take place each week. (http://www.cnn.com/2001/TECH/internet/05/24/dos.study.idg/index.html) With the amount of attacks taking place, users need to take action to protect their computer data and to prevent the use of their systems in attacks against others.

What is a Trojan anyway?

The tech website **www.whatis.com** defines a Trojan with the following:

> "In computers, a Trojan horse is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and do it's damage, such as ruining the File Allocation Table on your hard disk."

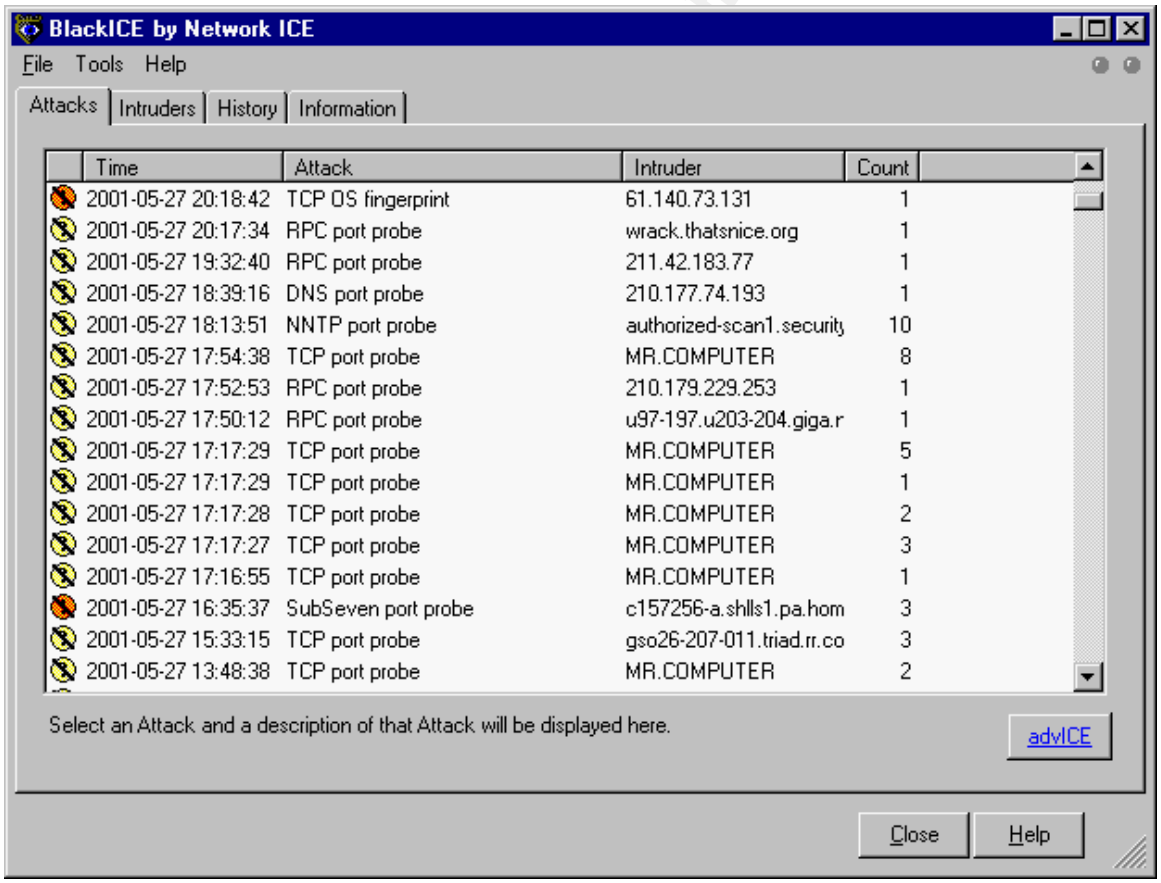
In the examples given above the hackers were not concerned with attacking the individual users machines. The Trojans were instead used to take control of a user's machine and Turn it in to a Zombie. A zombie is a compromised machine that is used to carry out denial of service attacks against other sites or machines.

Once a hacker has control of your system, he is free to use it as he sees fit. The hacker can install programs, delete files, send messages, and carry out attacks on others.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Am I really at risk?

Recently I moved to cable modem access. After reading all the stories about DDoS attacks and compromised home computers I wanted to see if the volume of attacks was accurate, and to see if unscrupulous hackers really were interested in my system. As a test I set up one of my machine with Windows NT workstation 4.0 and installed Black ICE defender, a personal firewall and intrusion detection application that I had heard about on Tech TV news. I than connected it to the cable modem. It should be noted that I do not specifically recommend Black ICE Defender as it has numerous limitations (for specific information on these limitations see www.grc.com), it is used here as it does contain one of the most easily understood logging facilities of the current personal firewalls. Within hours I had numerous attempts to scan and access my system as shown by the screen capture below.



You will notice that on the date of 2001-05-27, between the hours of 1:48pm and 8:18pm BlackICE logged 16 unique attempts to access my machine. As shown by the count column, some of these attacks were tried multiple times. The types of attacks varied from a simple TCP Port ping to a scan for the Subseven Trojan.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The intruder listed, as Mr.Computer is one of my machines that I used to scan the machine running BlackICE from my internal network. The intruder listed as authorized-scan1.security is actually authorized-scan1.security.home.com, my ISP scans port 119 for Network News Transfer Protocol (NNTP) as running a newsgroup server is a violation of the Acceptable Use Policy (AUP).

To see if your computer is inflicted with a Trojan you can run netstat -an at your command prompt. The –a parameter displays all connections and –n displays the addresses in numerical form. Netstat will list all open ports on your system including legitimate connections. Netstat will not show what application is using each port, but you can compare open port's to a list of know Trojan ports at http://www.doshelp.com/trojanports.htm. For example in the past ports 6711 - 6713 were known to be ports for the Subseven Trojan. The known ports for certain Trojans are a good place to start, but many Trojans are now able to use any port, and as a result it is better to use netstat to look for any unexpected traffic. In addition to netstat, you can also use a port scanner to determine open ports, many are available at http://www.cotse.com/tools/pscan.htm. If you are using Windows NT or 2000, Foundstone.com has a free utility called Fport that will map open ports to applications.

Below is a sample of netstat's output.

Active Connections

Proto	Local Address	Foreign Address	State
TCP	computer:1078	MR.COMPUTER:0	LISTENING
TCP	computer:1027	cs8.msg.yahoo.com:5050	TIME_WAIT
TCP	computer:137	MR.COMPUTER:0	LISTENING
TCP	computer:138	MR.COMPUTER:0	LISTENING
TCP	computer:nbsession	MR.COMPUTER:0	LISTENING
UDP	computer:1078	*:*	
UDP	computer:nbname	*:*	
UDP	computer:nbdatagram	*:*	

How do Trojans arrive on my system?

The most common ways to have your computer infected by a Trojan are as follows:

Email:

The Trojan arrives as an attachment disguised as a useful program or even embedded inside another program.

Theoretically with the advent of self-executing viruses such as Melissa, the Trojan could potentially deploy itself without the user consciously executing it. In the case of the

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Melissa virus and Microsoft outlook, Melissa was written in Visual Basic script, which Outlook will execute in the preview pane by default.

Local Installation:

Someone could potentially install a Trojan while physically sitting at your machine, from a floppy disk, CD-ROM, or other removable media. For example: even if you have a screen saver that locks your computer with a password, anyone could insert a CD in your CD-ROM and have it automatically open the CD and install programs.

Web Sites:

A Trojan could also be installed from a website through a malicious Active-x or Java applet. Java and Active-x code have the ability to execute programs off of a website as if it were installed locally on your computer. In the case of Active-X, the programs execute locally on your system with full administrative privileges.

A Trojan could also be hidden on a website in a file that appears to be a useful program. For instance, you download the newest free game, Elf Bowling 12 and play. While unknown to you, it is secretly transferring files from your pc to a server on the Internet or worse; it's using your Internet connection to flood the connection of another user or site.

What can I do to prevent my machine from being used as a Zombie? Isn't virus Protection enough?

In recent months some Trojans have been reclassified as remote administration tools. The most glaring example is Back Orifice. Many Trojans are also purposely taking steps to hide themselves from anti-virus tools. And as a result you should not rely on an anti-virus tool alone. Instead you should practice the philosophy of defense in depth, by utilizing multiple security tools and minimizing actions that could put your system at risk.

Email:

1. Ensure you are running the latest version of your preferred email client.
2. Disable any auto preview features on your email client.
3. Do not open attachments if you cannot verify the origin of the file as having been sent from a source you trust.
4. If you run Microsoft Outlook, install the attachment security update from the following site: http://www.microsoft.com/PressPass/press/2000/May00/SecurityUpdatePR.asp
5. Disable any scripting features, to prevent any hidden scripts from executing.

Local Installation:

1. Ensure that you do not access disks unless it is from a trusted source such as prepackaged software.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

2. Disable the auto run feature of your CD-ROM drive. Instructions for disabling auto run in Microsoft Windows can be found at the following URLs http://support.microsoft.com/support/kb/articles/Q126/0/25.asp or http://msdn.microsoft.com/library/psdk/shellcc/shell/Shell_basics/Autoplay_reg.htm

3. When you are away from your machine protect it with a password.

Web Sites:

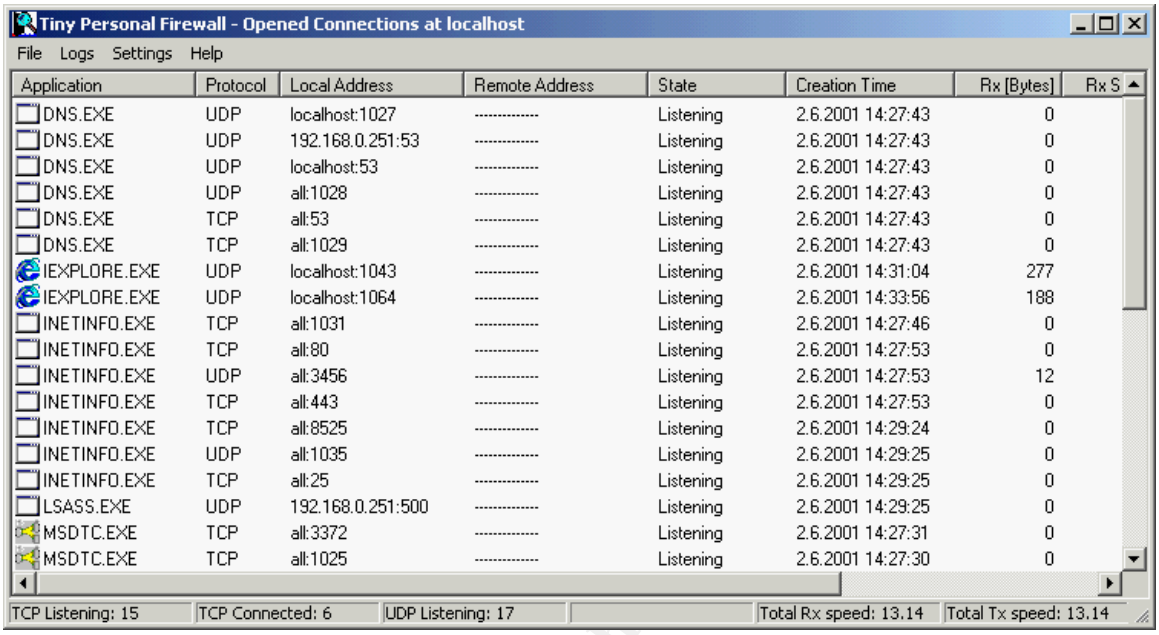
1. Enable Active-X and Java filtering in your web browser.
2. Run a virus protection application such as McAfee Virus Scan that protects against malicious Active-X and Java applets.
3. Scan all downloaded files with a virus protection application.

Firewall:

1. Install and run an application level personal firewall. Also try to use a Firewall such as Tiny Software Personal Firewall (available at www.tinysoftware.com, free for personal use) that uses an encryption algorithm such as MD5 to verify that any application allowed through has not been modified. As of this writing the only two firewalls that are know to perform application integrity checking, they are Zonelabs' Zonealarm (www.zonelabs.com) and Tiny software's personal firewall. Test the firewalls encryption support with the Leaktest application available at www.grc.com.

   Some firewalls provide a facility that will show what ports are open and the particular application that is using them. Below is a screen capture of another useful feature of Tiny Personal Firewall's Status Window. As you can it is a very useful feature that maps all open ports to applications. I have not found any other firewall product that implements this functionality.

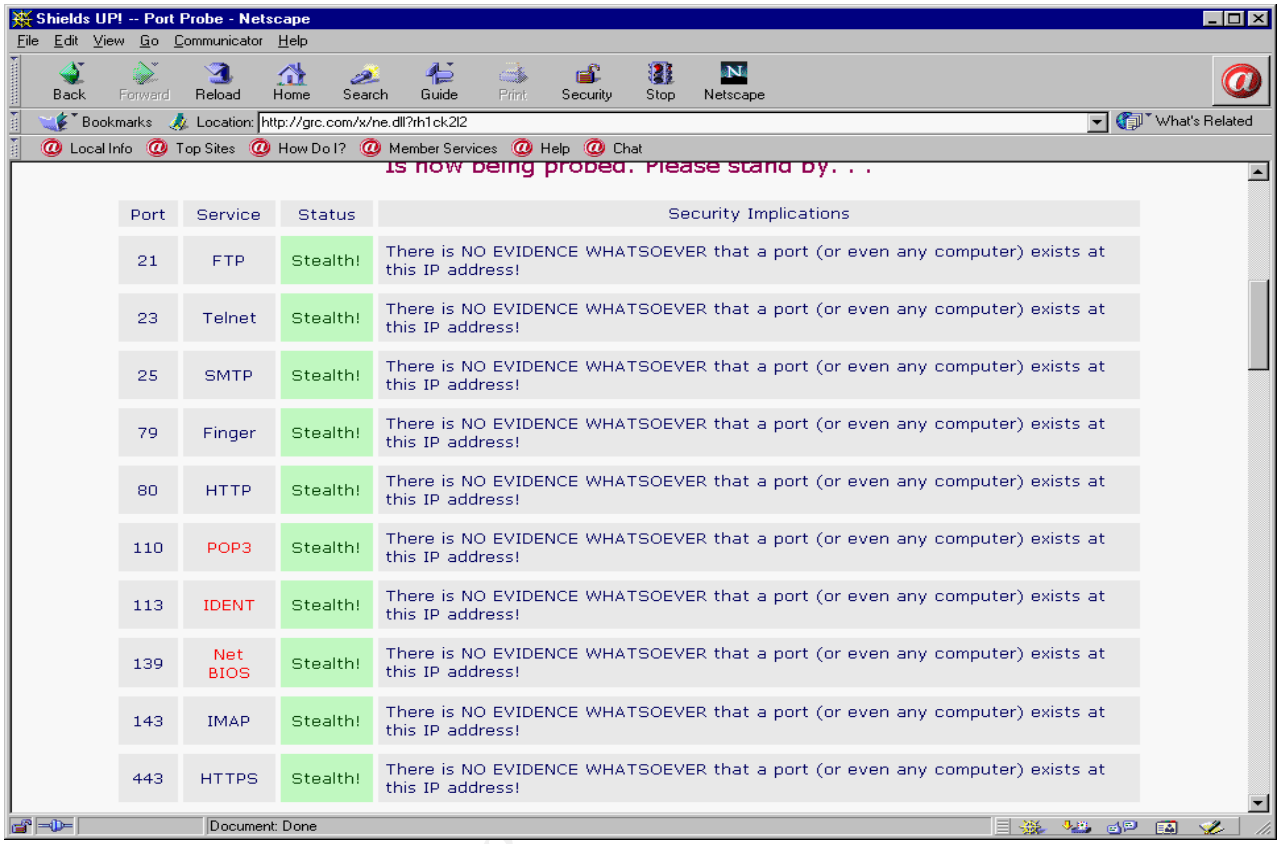
© SANS Institute 2000 - 2002 Author retains full rights.



2. Ensure that your firewall logs both incoming and outgoing traffic.
3. Periodically check your firewall with security tests such as Shields Up at www.grc.com and http://www.dslreports.com/scan. Below is sample output from both tests.

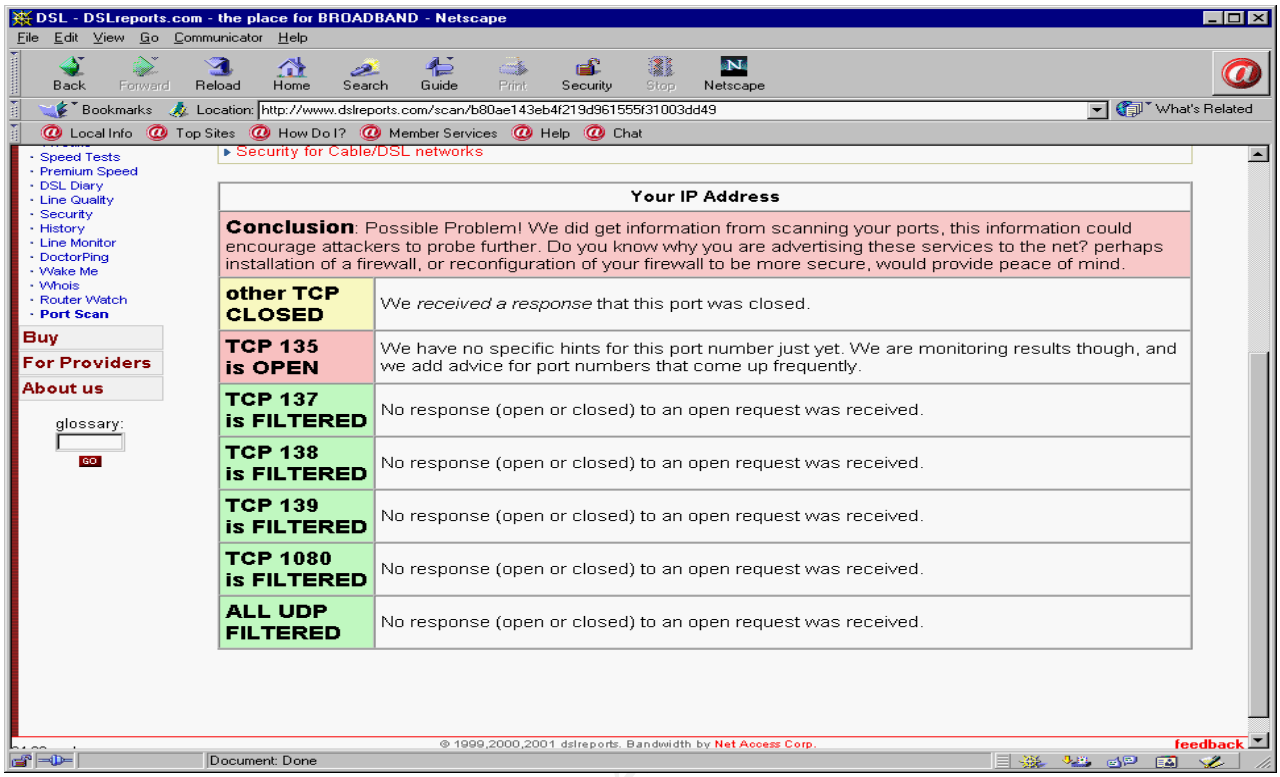
Grc.com Shields Up: With this service, you should ensure that you do not have any ports listed as open. Be aware that even if your machine is listed as not having any ports open you should not feel that you have no security concerns, as Shields Up! only scans 10 ports of the total 65535 TCP/IP ports.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.



DSLReports.com: The free version of Dslreports security scan executes some common attack scripts that hackers use against your firewall in addition to scanning 2086 ports including all 1024 of the well-known ports. Information on the paid version can be found at http://www.dslreports.com/secure_features.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.



MD5 encryption sounds great, but how does it work?

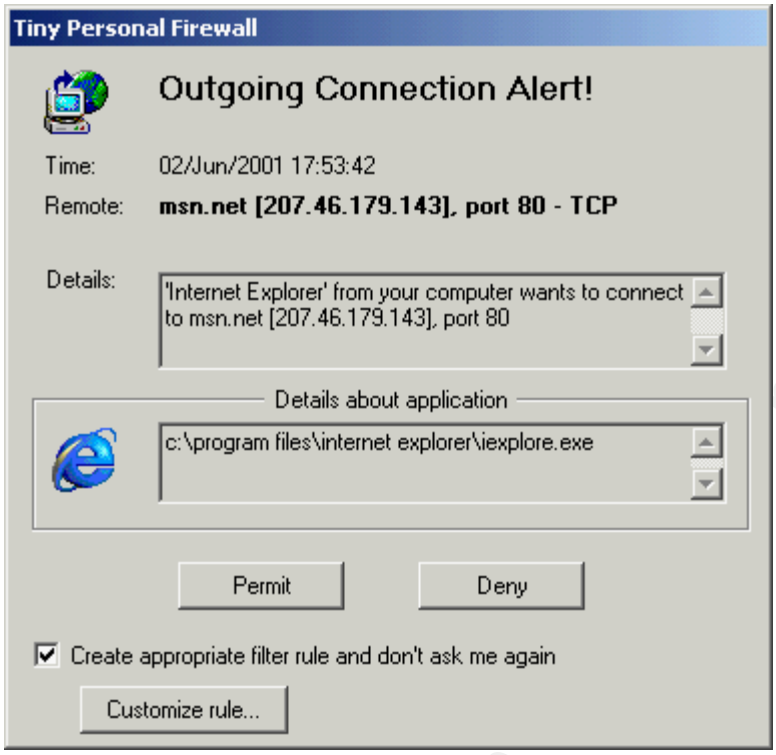
MD5 is an acronym for Message Digest Algorithm and was developed by Ron Rivest, and is now owned by RSA (www.rsa.com). RSA is well known for their implementation of the triple DES algorithm. MD5 is the third version of the RSA MD algorithm. The MD algorithm was originally developed to allow messages to be sent securely back and forth between recipients, ensuring any third parties did not alter the contents.

MD5 is a symmetric key block cipher algorithm, meaning it encrypts data in 512- bit blocks and outputs a single 128-bit "message digest". MD5 does this by separating the data into 512-bit blocks. If the data ends with less than a 512-bit block, the algorithm "pads" the data by adding extra bits until it is a full 512-bit block. Next MD5 applies a 64 –bit representation of the original data to the end of the padded data. Third MD5 initializes the MD (message digest) buffer and with 4 predefined 32-bit register values. Fourth, MD5 applies its encryption algorithm to each block. As a result, each file should have it's own unique signature. The precise workings of each MD5 step are beyond the scope of this paper. To read about the process and view the algorithm, see RFC 1321.

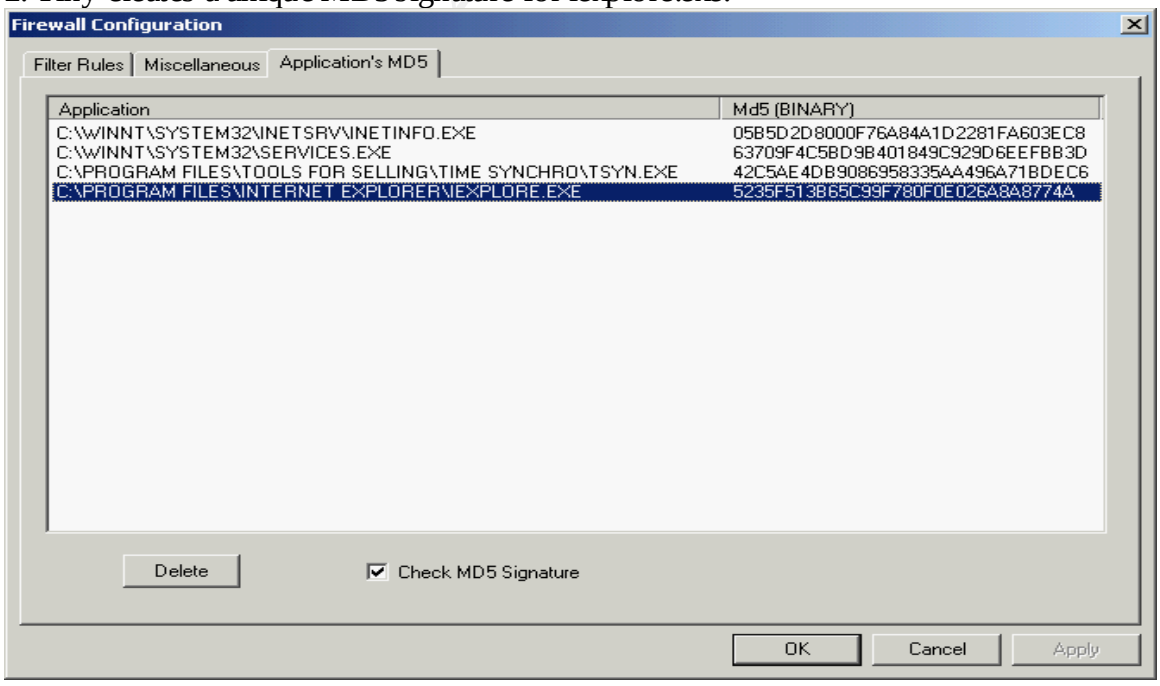
The benefit to this technique is that it should be virtually impossible for any program to impersonate another program. This behavior when implemented properly in a security product will also prevent non-registered programs from traversing the firewall to the Internet. An example of how Tiny Personal Firewall uses the MD5 signature is below.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

1. First we configure Tiny firewall to allow Internet explorer (iexplore.exe) to access the Internet. As shown below.

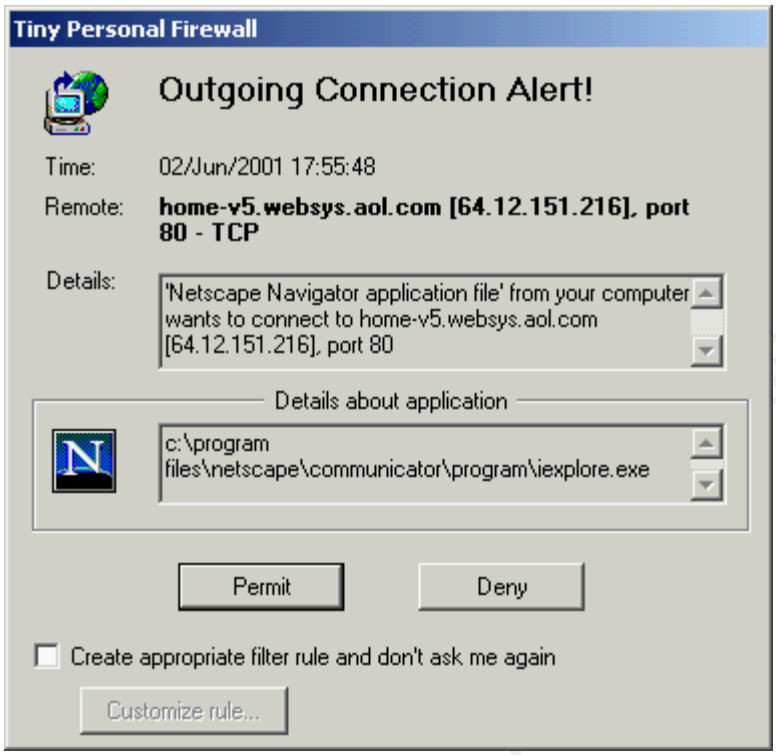


2. Tiny creates a unique MD5 signature for iexplore.exe.

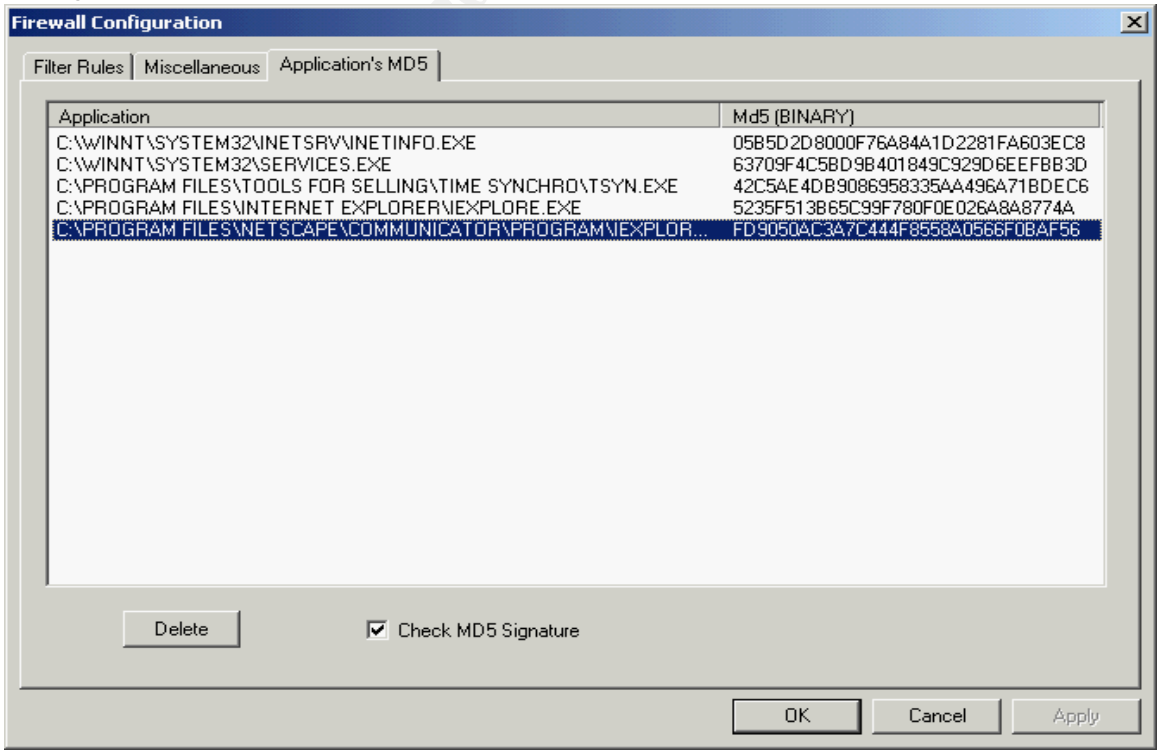


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

3. To test the MD5 signature, I renamed netscape.exe to iexplore.exe, and tried to access the Internet. Tiny blocked the renamed netscape.exe as shown below.



4. Next I viewed the MD5 signature window to verify that Tiny did in fact create a new signature for the renamed netscape.exe. As you can see, both filenames are identical, but the MD5 signatures are different.



© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Summary

Even though no "silver bullet" solution exists to stop personal computers from being used as zombies, you can effectively minimize this abuse. Utilizing a firewall on your computer, and following these simple prevention tips you can minimize the risks of having your computer or computer's you manage used as a zombie in attacks against others.

References

Avert Research Center
http://www.mcafeeb2b.com/naicommon/avert/avert-research-center/default.asp

Costello, Sam. "Study: Nearly 4,000 DoS Attacks Occur Per Week"
http://www.cnn.com/2001/TECH/internet/05/24/dos.study.idg/index.html

COTSE
http://www.cotse.com/tools/pscan.htm

DoSHelp.com :Intrusion & Attack Reporting Center
http://www.doshelp.com/trojanports.htm

Gibson Research Corporation
www.grc.com

Microsoft TechNet
www.microsoft.com

RFC 1319 & 1321
http://www.cis.ohio-state.edu/cgi-bin/rfc/rfc1319.html
http://www.cis.ohio-state.edu/cgi-bin/rfc/rfc1321.html

Symantec AV Center
http://www.symantec.com/avcenter/

System Administration and Network Security Institute
www.sans.org

Tiny Software Company
www.tinysoftware.com

"What are MD2, MD4, and MD5"
http://www.rsasecurity.com/rsalabs/faq/3-6-6.html

Whatis?com
www.whatis.com

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002, Author retains full rights.