Global Information Assurance Certification Paper

Vincent Wallace

Personal Firewalls: Not Enough

With the proliferation of residential broadband more and more users are able satisfy their craving for always-on Internet access. As the subscription to DSL and cable services grows, so does the size of the playground for malicious users. Many subscribers to these services are unaware of the problem and others think that they are not a target. For many, however, the problem is real and they are taking steps to protect themselves.

The hot technology of the day for broadband users to combat malicious attacks is personal firewalls. There are about a half dozen on the market and rest assured more are on the way. Most personal firewalls are designed to protect users from malicious incoming attacks, identifying suspicious packets, logging and/or notifying the user of the activity and dropping the packet to keep the computers presence on the Internet hidden. A large subset of these programs also protects the user by prohibiting rogue applications from accessing the Internet without their permission. However, in the rush for companies to seize market share, not all of these security tools are completely protective.

The Problem

The problem, originally reported by Steve Gibson of Gibson Research Corporation, is that almost all personal firewall software includes a list of well known "trusted" applications that are allowed to access the Internet without question (3). These applications, such as web browsers, ftp software, etc., are allowed to pass their traffic through the personal firewall software without prohibition. This behavior seems relatively benign, because most users would like for their personal firewall to provide them with security without completely blocking their access to the Internet. The problem, however, lies not with the fact that the firewalls, in most cases by default, allow traffic from trusted applications to pass through the firewall, but with how these firewalls identify the trusted applications.

It has been discovered, by Gibson and confirmed by several others, that almost all personal firewall packages use similar methods for identifying trusted applications: executable name, and in some cases also by the ports that the application typically utilizes. This allows even the most junior malicious user to change the name of a harmful well known malicious tools to that of a common trusted application, deliver it via a Trojan horse to a users computer, and completely bypass his or her personal firewall. This is not a difficult attack and it is a very real threat.

To demonstrate this inherit security weakness in personal firewall software Gibson created a simple application, called LeakTest (4) that masquerades as a popular application that is trusted by default by most personal firewall software. LeakTest sends a test packet to one of Gibson's servers, to test that the application successfully bypasses a personal firewall, and sadly, in most cases on most personal firewall software that is exactly what happened. While Gibson's utility claims to be harmless (can anyone ever be sure) it is a rude awakening to personal firewall software makers and users, and opens the door for many more malicious possibilities. In fact Jim Williams of About.com (5)

was able to simply rename the Back Orifice executable to that of a popular web browser, and most of the personal firewalls currently on the market allowed Back Orifice's traffic to pass through without warning.

To further complicate the issue some personal firewalls are not only subject to this activity, but will also allow applications to insert new rules into the firewalls filtering engine. This allows a malicious executable to not only bypass the personal firewall, but also to modify the firewalls rules, opening the door for more insidious attacks (3).

Should You Be Concerned?

Some security experts seem unconcerned by this potential threat, saying that "worrying about it is like worrying that your car will be hot-wired when you've left the doors unlocked and the keys in the ignition" (2). This view seems very narrow considering the rash of recent wide spread attacks that have plagued the Internet community. For example the distributed denial of service attacks that crippled several major companies' Internet services, or the wild fire spread of e-mail viruses like Melissa and ILOVEYOU.

People use personal firewalls to protect themselves from being attacked by malicious users, and the use of such software can help prevent the growing population of broadband users from being effected by or hosting the next plague that will surely come. Saying that a way to render personal firewall software ineffective is minor and not an issue is simple challenging the cracker community to prove the naysayers wrong. Personal firewall software is not a magic bullet to solve every security need, but it is a cornerstone to the security wall that protects users from the evil of the world.

Company Reactions

In standard form most companies that make personal firewall software reacted with the usual we will rush a patch to our website within the week. Other companies indicated that they would be releasing a new version of their product soon that incorporated a fix to address this security hole. This is a nice way for these companies to save face, however it was rushing their products to market that caused this relatively simple breach to be a problem in the first place.

The most amusing response came from Network ICE, the makers of BlackICE Defender. They stated that while their product was only designed to address attacks from external sources, it would protect against known malicious programs. Network ICE's executive's sited that should a product such as Back Orifice 2000 be used in such an attack BlackICE Defender would recognize the attack because it would recognize the encryption patterns of the malicious software (3). However in his test, Williams (5) used a renamed Back Orifice executable to punch right through BlackICE Defender.

One other notable response to this new security threat came from Zone Labs, makers of Zone Alarm and Zone Alarm Pro. Despite the fact that their products actually

stopped both Gibson's and William's tests their response was that no security product is one hundred percent safe. They realize that even though they were successful this time, they may not be the next.

The Fix

So why did Zone Labs' products do so well while others failed? Zone Labs did two things differently. First, the default policy for their products are that no traffic is allowed through from any application until the user grants that specific application the privilege to send and receive traffic through the firewall. This helps prevent the malicious program from sending data without the users knowledge, because the user must specifically grant the application that privilege. Most of Zone Labs' competitors either pre-populated a trusted application list, or used the completely opposite method of allowing all traffic from all applications to pass through their firewall software until specifically denied by the user. They therefore on the users behalf made an assumption of what programs the user may or may not be running and gave those programs access to the internet by default without the users knowledge. Zone Labs' method of deny all works nicely if the malicious code is renamed to a program that is not currently granted access to the Internet, but what happens if the malicious code is renamed to a program that has been granted access to the Internet.

This is where Zone Labs again differentiated itself from its competitors. Unlike its competition Zone Alarm and Zone Alarm Pro do not rely strictly on executable names and/or utilized port numbers to identify a trusted application. Once an application is added to the trusted programs list an MD5 hash of the application is stored in the rule base (3). This means that in order for a malicious program to successfully masquerade as a trusted programs and breach Zone Alarm's or Zone Alarm Pro's security it would have to have an MD5 signature identical to that of the trusted executable. While it is not impossible for two applications to have the exact same MD5 hash it is statistically improbably. By taking the small step of storing an MD5 hash of the programs executable Zone Alarm and Zone Alarm Pro were able to identify that a renamed malicious program was different than a trusted program by the same name.

Needless to say most other personal firewall companies have announced that they will be changing their products to incorporate MD5 hashing as a way to identify trusted programs (3). Others also are changing their minds on pre-populating the list a trusted applications in their products (5), and some are also changing the default behavior of their software from allow all traffic to deny all traffic. Changes such as these will inconvenience many personal firewall users because they will now have to be more aware of proper configuration of their personal firewall software and will no longer be able to set it and forget it.

What Else Can Be Done?

While more careful product development by the companies who make personal firewall software could have easily prevented this form of firewall subversion, in the real

world such an attack could have still been prevented. The key to successful security is defense in depth, at work and at home. Home broadband users have a myriad of tools available to them to protect their computers. While personal firewalls are a main ingredient to defense in depth, anyone who is concerned with his or her personal computer being compromised should not rely on only one form of defense, and should make use of as many of the available tools as practical. In most cases depth of defense can be achieved with a minimum cost and effort.

A primary defense against an attack on personal firewalls such as the one discovered by Gibson is file integrity checking. File integrity checking is the process of verifying changes, additions, and deletions to a computer's file system. This can easily be achieved utilizing tools built into most operating systems to record critical information about files such as size and date. Another method is to use a file integrity checking utility. These utilities not only record this critical file information but also use cryptographic hashes of files to increase certainty of file integrity. This method of security could have notified a user of a compromise to the system, because the malicious code would appear as an addition or modification of a file or files on the system.

Another technology that is becoming more and more popular in the home is small workgroup sized routing switches with built in firewall and network address translation (NAT) capabilities. Many homes, when subscribing to broadband services, set up small LANs to allow other members of the household to access the Internet from various locations within the home. While this technology may not have prevented the malicious code from infecting a target system, it could help keep damage to a minimum. These devices can achieve protection in two ways. First, the built in hardware firewall capabilities are not as easily compromised by this style of attack. They do not use a list of trusted applications to dictate what applications are allowed access to the Internet and therefore would not allow a renamed malicious program to send an receive traffic based solely on name, nor would they allow such a malicious programs to open new ports for traffic to pass through. Secondly, since most utilize NAT technology the private IP address of a compromised computer would be hidden from an attacker because all internal traffic from the NAT environment is translated to the switching router's public IP address. This leaves the would be attacker with no way to address the target computer behind the protection of the NAT.

Access controls are an underutilized security tool in the home user market. While many operating systems marketed to the home user audience do not have access controls built in, they are incorporated in majority of non-home user targeted operating systems, which are slowly beginning to penetrate the home user market. Access controls limit where and how users can access a computer's files. In the scenario of a Trojan penetrating a system, access controls could prevent the unwitting user from allowing the Trojan to deliver its payload by not allowing the user to access the area of the file systems where the Trojan is targeting. Since the firewall subversion attack discussed would be delivered via Trojan, access control tools could prevent this form of attack.

Something many home users do currently utilize is one of the many virus scanning programs available. A good up to date virus scanner could have stopped a malicious program from being delivered via Trojan and thus stopped the subversion of the personal firewall software. Virus scanners and up to date virus definitions are critical to preventing security breaches.

Possibly the most important element of security in depth is education. As stated earlier the most notable viruses and Trojans of late have been spread inadvertently by uneducated users. Viruses such as Melissa and ILOVEYOU did significant damage and they should have been a wakeup call to anyone that uses a computer that they need to learn more about the threats and vulnerabilities to and of their computers.

Conclusion

Personal firewalls have become a primary method of defense for the growing population of home broadband access users. They provide a much-needed defense mechanism against the growing number of threats on the Internet. However, personal firewall software is not a total solution, and they like all software are prone to attack. However, by not relying solely on a personal firewall as a single line of defense, system compromises that could subvert personal firewalls can be prevented and/or the damage they do can be minimized.

References

1. Berinato, Scott. "Personal firewalls not so safe." eWeek. 11 December 2000. URL: http://www.zdnet.com/eweek/stories/general/0,11011,2663028,00.html (10 February 2001).

2. Rapoza, Jim. "Labs'-eye view." eWeek. 11 December 2000. URL: http://www.zdnet.com/eweek/stories/general/0,11011,2663030,00.html (10 February 2001).

3. Captain, Sean. "Firewall makers scramble as security gadfly exposes flaw." PC World. 12 December 2000. URL: http://www.itworld.com/Sec/3833/ITW3710 (10 February 2001).

4. Gibson, Steve. "Internet Connection Security for Windows Users." Gibson Research Corporation. URL: http://grc.com/lt/leaktest.htm (10 February 2001).

5. Williams, Jim. "Personal Firewall Security Hole." About. URL: http://www.netsecurity.about.com/compute/netsecurity/library/weekly/aa121200a.htm (10 February 2001).

Last Updated: July 25th, 2017

Upcoming Training

SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
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