Global Information Assurance Certification Paper

Security risks and countermeasures for home users.

Ireen Birungi
Ver.1.3
February 15, 2002
Revised April 3, 15, 2002

ABSTRACT

From processes and guidelines to software applications, information security has almost exclusively focused its efforts on securing large organizations and corporate communities. What about the simple home user, or the traveling businessman that ventures past the "safe" confines of their internal networks? How does one ensure they can minimize their risks from the ever-present threats on the Internet?
There are tools available to help secure the mobile or home computer, many of which are free, that can mimic a defense in depth strategy employed within a corporate environment. For example, instead of introducing a network-based firewall into your home, one can simply install a small piece of software called a "personal firewall" that will perform nearly identical functions. Also, to prevent virus infections one does not need to deploy a gateway virus scanner. Personal anti-virus software will perform nearly identical purpose.

Are these preventive measures enough to completely secure personal data? Not likely. As security software grows more sophisticated, so to does the sophistication of attacks. Recently a virus was found in the wild, the Goner virus, that when successfully infecting a system, it would attempt to disable personal security software such as anti-virus scanners and personal firewalls. This can potentially undermine all the proactive steps taken by the user leaving them vulnerable to further attacks.

The question then shifts from "how can I secure my data?" to "how can I best minimize my risks?" Is it possible to be completely "safe" on the network of networks? There will never be a definitive answer to this question. It will always be an up hill struggle, but by implementing industry best practices and keeping current with security news one can stand a fighting chance.

Many corporations are focusing a lot of their efforts on the security of customer information in transit during e-commerce transactions or stored within their corporate networks. Security has become even more important since the much publicized unavailability and vandalism that many credible sites have been subject to. This leads to financial loss resulting from down time in productivity and data loss. Computer Security Institute (CSI) reported "Eighty-five percent of respondents (primarily large corporations and government agencies) detected computer security breaches within the last twelve months." [1] Of these respondents, $377,828,700 was the reported financial loss. Unfortunately, these figures don't represent the true total dollar loss. It only represents the companies that were courageous enough to report to being attacked.

Most of the security related incidents reported that affect end user machines are malicious code introduced through many avenues such as email, Internet, programs, and floppy disk. "We are living in an increasingly connected world, which brings a higher risk of outbreak and faster spread".[2] Malicious code interacts with the machine to produce undesirable behavior. It may come in the form of viruses, worms, Trojans, and harmful mobile code such as activeX and Java applets. It is estimated that in 2001 the total damage caused by malicious code attacks was $13.2 billion.[3] These figures reported are pretty scary but very realistic and once again represent only the companies that were brave enough to report these incidents.

In the past attackers would have to attempt to penetrate the network perimeter of an organization in order to gain access to corporate data. That is no longer the case. Mobile corporate users that bring their work home are much easier targets. The attacker no longer has to work hard at gaining access to the corporate information stored in the organization, instead the corporate information is stored on a machine that is connected to the Internet from home. For this reason, it is important that home users connected to the Internet are adequately protected. This paper will provide details to explain the security software solutions that are available for home protection, what they do, and how they differ. It will provide a brief insight into the next generation of personal security software. Moreover, it will present a summary of the Goner virus that threatened the existence of security software.

What is Anti-Virus?

Most computer users are often advised to install virus software in order to protect their machines from the harsh world of the Internet and its wealth of malicious software. Often times this protection is to ensure that personal data is not lost, compromised, and that the computers are not made unavailable. Personal data may include address books that contain personal information such as first and last name, home telephone numbers, addresses, which are precious commodities to marketing firms, passwords, accounting information such as expenses, liabilities, assets, and balances, and small client database for small businesses. But what does anti-virus really do.

Viruses, worms, and Trojans are written with the intent of wreaking havoc to vulnerable systems and networks. Just like you have delinquents that like to vandalize buildings and train carts with graffiti, the same exhilaration is experienced when a system has been compromised due to a virus payload. Anti-virus software acts as a countermeasure or graffiti repellant paint in order to detect and protect against viruses, worms, and Trojans. They are programs that search files or computer memory for the presence of a known virus. This is accomplished through the use of a database of signatures, usually found in a virus signature file. This signature provides virus information to the engine , which in turn makes a decision to take the appropriate action based on the configuration of the software. Figure 1 presents what is typically found in a signature file, in this case the Goner virus signature. A signature is comprised of unique letters and numbers that are found within the code of a virus. The anti-virus software engine compares found strings in infectious attachments using the characters found in the signature file. If the letters and/or numbers of the virus match the contents of the signature file, a virus has been found. The engine then responds by either prompting the user for an action, deleting the infected file, moving the infected file, cleaning the infected file or denying access to the infected file.

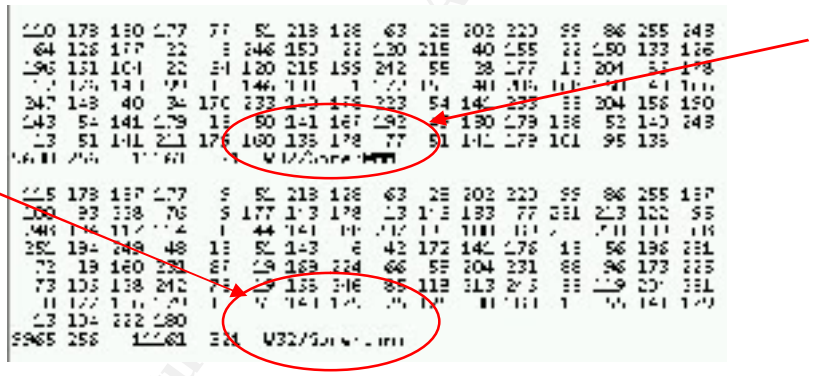

Figure 1 Virus Signature of the Goner Virus

Signature file provided by Network Associates

A downfall to anti-virus software is its inability to quickly detect new viruses in the wild; this is under the assumption that the anti-virus software is frequently kept up to date. Viruses are spreading quickly and often times slip past traditional anti-virus software before the vendor can distribute the appropriate update file. These update files update the anti-virus software detection engine in order to detect a virus and protect the user's machine. Sometimes this can prove to be too late as it provides a "window of vulnerability between the first release of new viruses and the time a user updates their"[4] virus signature engine. It is for this reason that the anti-virus software industry is moving to anti-viral software that detects malcode based on behavioral patterns, also known as anomaly based software. The behavioral pattern software integrates with the machine at an operating system level to monitor program behavior for malicious activities before affecting the system. When it detects that an executed program is exhibiting malicious

behavior, it responds by blocking or terminating the aggressive program. The activities that are monitored may include:

- Attempts to open, view, delete, and modify files
- Attempts to format disk drives and perform other disk operations
- Modifications to executable files, and macros scripts
- Modifications to system settings
- Initiation of network communications,

There is still quite a bit of research in this technology being conducted, however, if it works in the way that it is intended, it will be a break-through in malicious code detection, prevention, and will provide user protection.

Personal Firewalls

A firewall is essentially a program or device that provides protection between two networks. In most scenarios it is deployed between the inside walls of a corporate network and the Internet. It is controlled through the configuration of a rule base, which determines the fate of the data. This data, when dissected, is broken down into packets. Most companies deploy what is called a network firewall, which can be software installed on a number of operating system platforms or deployed as a device. These commercial network firewalls have proven to be expensive for the average user and it is for this reason that software personal firewalls have become very popular amongst home users. They are cost effective, sometimes even free, and fairly easy to install, configure, operate and support. The target users that personal firewalls aim to market are home users, corporate users who use their laptops at home to connect to the Internet, laptop users, and small businesses. Like anti-virus software, personal firewalls are used to protect personal data from the prying eyes of Internet attackers. They are a "software-based solution's safeguard against hackers".[5]

Users that are at most risk are those that have high speed Internet connections using Digital Subscriber Line (DSL) or cable modems because they most often maintain a persistent connection to the Internet. Dial-up modems share the same risks, however, on a smaller scale. This is because there is usually a connection timeout (disconnect) after a certain amount of idle time. In dealing with Internet access, the assumption can't be made that the network, which the ISP has provided, is appropriately protected at the network perimeter points. Sure they may have firewalls in place, but they have to accommodate customer business requests, otherwise they wouldn't be in business. In fact most ISP's do not provide packet and content filtering for customers accessing the Internet. This means that there are a large number of port accessibility points in which malicious code and attackers can take advantage of. A common example of this is through the use of Trojan programs. You download a game from the Internet that is accessible via port 80. That's pretty standard. The game is installed and rather than

being the game that you thought you downloaded it is equipped with a Trojan that creates a back-door to the Internet, which in turn gives access to a remote attacker. The communication between the attacker, who will broadcast packets to the Trojan program for a response, and the Trojan server program will occur on whichever port that the attacker has authored. A perfect example of this is Back Orifice (2000) also known as BO2K, which listens on TCP port 54320, or SubSeven that listens on TCP port 27374. These are their default ports but in order not to be detected they are configurable by the author to use whatever ports they desire. Many people have been victims of these attacks and to make it worse; there are websites on the Internet that provide information on vulnerable systems that have had Trojan's successfully installed. This makes it easier for other attackers to find the identified machines and hack away.

Personal firewall programs come in two types: Packet-filtering and application layer. They are both software based and can be installed directly on the operating system. Packet filtering firewalls, as the word implies, filters data packets at the data level. It examines the data packets entering or exiting the user's machine through an Internet connection and makes a judgment on whether to accept or deny the packet based on-information such as Internet Address (IP) source, destination and port number. A good example of a personal firewall that uses this firewall method is Network ICE's BlackICE Defender (http://www.iss.net/). Depending on the rule base, any communication that is detected to be hostile or does not seem normal behavior, for example the user will be notified by the software when packets try to connect on a port that strict access controls have been applied. The packet will be dropped, and the request will be logged. Packet filtering configuration is essential because access controls for data packets rely on the rule definition. A bit of technical knowledge will have to be consulted in order to properly configure the software.

Application layer firewalls analyze data communications at an application level. When a program such as SSH client wants to communicate with a remote server, the application resorts to its policy and checks to see the privileges set against that application. If any permission controls exist, the firewall will respond by asking the user whether or not they would like that program to be given access to the remote application stating its IP address. The firewall also responds with an alert when receiving inbound and outbound requests that have not been authorized through the applications configuration and maintains a log of requests to and fro the machine. An example of application layer personal firewall is ZoneLab's Zone Alarm (http://www.zonealarm.com/).

Both these types of firewalls are a great investment in time and costs and provide another layer of security. They will be able to provide information on inbound and outbound connections at a data or application layer. This way you can track malicious activities such as Trojans communicating successful infection to the author or responding to a request by an attacker.

Higher assurance with personal firewalls

There are other types of personal firewalls that will provide higher security assurance and are set apart from software-based firewalls. They are called personal firewall appliances. They are a hardware solution typically used in small businesses, home office, and small network type environments. These hardware-based solutions are separate devices that are connected to the network perimeter of a user's home office, small business, or network. A good example of this type of personal firewall is Netscreen's Netscreen-5 (http://www.netscreen.com/products/appliances.html#ns5xp) and RapidStream RapidStream 500 (http://www.rapidstream.com/pdfs/RS500_datasheet.pdf). These types of firewall solutions provide:

- Network Address Translation (NATing) in order to hide the addresses of internal hosts. This implementation is directed to small businesses that have their own Internet address ranges. Packets originating from internal hosts are seen to have one address.
- Provides a VPN capability
- Strong encryption
- Built in Intrusion Detection, which monitors behavior of traffic against attack signatures
- Strong authentication
- Stateful packet filtering
- URL or content filtering i.e. JavaScript, Java applets
- Automated alerts via email and SNMP traps

In order to configure the appliance, a browser like Netscape or Internet Explorer is used to access the configuration application or the appliance will provide a proprietary browser based tool. The user is required to log into the firewall in order to configure and view log files. Personal firewall appliances provide strong security to protect information assets against threats and are highly recommended for users that store highly confidential or sensitive information.

Although current industry best practices (anti-virus and personal firewalls) have been implemented, they do not necessarily eliminate the risks. The description reported on December 04, 2001 about the Goner virus provided information on how this virus threatened the existence of security software by attempting to delete security software off a user's machines and in many cases managed to compromise systems. The virus attempted to delete the anti-virus and personal firewall software installed on the machine, making it vulnerable to other attacks. Stephen Northcutt says it best when he states, referring to the hacking communities, that "they never cease to amaze me with their creativity."[6] Here is a brief description of what the worm does.

The GONER worm, also called W32.Goner, is a mass-mailing program written in visual basic script (VBS) that travels via Microsoft Outlook or Internet Relay Chat or mIRC in

the form of a screen saver. In order to spread, the worm must be executed and uses MS outlook to email itself to individuals found in the user's Windows Address Book (WAB). It also propagates via chat programs such as ICQ. Through ICQ it attempts to transfer files to users found in the infected machines contact list. When the user on the receiving end approves the file transfer, the worm then sends a copy of itself to recipients found in the address book. The worm also attempts to install a back door into the chat program and will use the infected machine to launch Denial Of Service attacks against the IRC server.

The original file size of the worm is 145 KB but reports a file size of 39KB. This is because it is compressed into a format called Ultimate Packer for eXecutables (UPX). UPX is a compression utility used to package executables. It not only reduces the size of a file, but also hides some character strings that would normally identify a file. UPX compressed executables, which may carry malicious software, are usually successful in bypassing current traditional anti-virus software because the signature file may not be deployed in time to detect the new malcode that is 'in the wild'.
When the attached file called goner.vbs is executed, a dialogue box is displayed as well an error message (see figure 2).

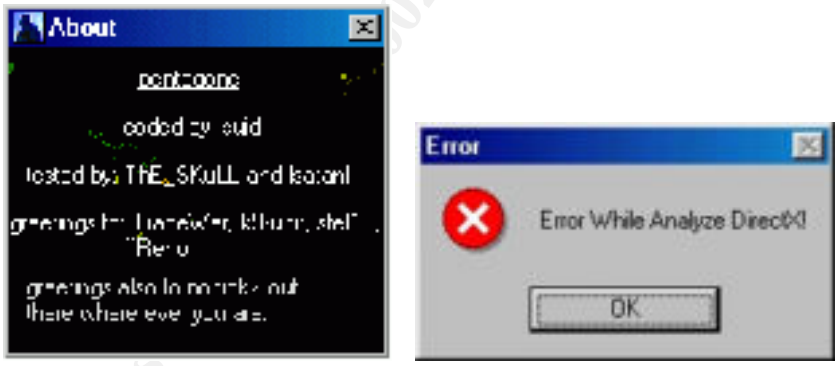

Figure 2 Dialogue Boxes of message displayed by Goner virus when executed.

Dialogue boxes have been provided by Network Associates.

As stated previously, the worm attempts to send itself to recipients found in the infected user's machine via MS Outlook. The message that the recipient receives is:

```
Subject:     Hi:
Body:        How are you?
             When I saw this screen saver, I immediately thought
             about you
             I am in a harry, I promise you will love it!
Attachment:  Gone.scr
```

After this, the virus rights to the Windows system directory and edits a registry entry to include the following line that will execute the worm after reboot:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\C:%WINDIR%\SYSTEM\gone.scr=C:\%WINDIR\SYSTEM\gone.scr

Once the registry has been added, the worm checks for common anti-virus and personal firewall processes in memory. If the process is found, the process is terminated as well as the corresponding executable file and directory components. This includes all files and sub-directories that are found in the program directory. As an indication that the worm has infected a machine, it deposits a file called REMOTE.INI, a process called goner.scr is listed, and on WindowsNT the taskbar shows an icon called pentagone. Some examples of the programs that are terminated by this virus are:
AVP (Kaspersky), McAfee VirusScan, ConSeal PC Firewall, eSafe, Norton Personal Firewall, Sophos, Lockdown Anti-Trojan, Norton AntiVirus, McAfee PC Firewall, Safeweb Privacy Software, Trojan Defense System, Trend Micro, and ZoneAlarm.

Other measures

As seen with the presence of such threats such as the Goner virus, anti-virus software and firewalls are not the only measures to combat Internet threats. There are other proactive measures that can be taken to further protect your machine. One of the most important measures is to be aware and stay informed about potential threats and possible solutions. High-risk viruses and vulnerabilities are usually reported in a timely manner through media channels such as television, radio, newspaper, credible Internet sites, vendor sites, and bug listings. Staying informed using any one of these channels would allow you to take proactive steps to ensure that your machine and personal data is protected. Also, it is not enough to have anti-virus software installed and expect that it will protect the system. Ensure that it is properly configured and that signature files and scanning engines are updated periodically. This is also true for personal firewalls. A firewall installed with its default settings may prove to be weak when protecting the machine from attacks. Once again stay informed on current vulnerabilities and bug listings and periodically check logs files for suspicious activities.

Other measures also include avoid opening email messages and attachments from people that are not familiar. In most situations, the message in the body of the email will say something inviting to encourage the receiver to open the attachment. In circumstances where the email comes from a person that is known to the recipient of the message, staying informed is one of the sure ways of being protected from infection. Many dangerous viruses that have been unleashed are written in visual basic script (.vbs) or arrive as executables (.exe). These types of files should be approached with vigilance. Run as few services as possible on the operating system, this is configurable in Windows2000/XP. Perform port scans occasionally. A good tool to use is nmap. This tool is available free for both Windows and Open Source systems. Lastly ensure that the product of choice fits the requirement. There are suitable software products on the market that are available to protect home computers. This should be considered when

researching about appropriate products. Firewall appliances are great investment for those small businesses that are engaged in high-value transactions. They provide more flexibility to apply stronger security controls to protect the network and customer information.

What's to happen?

The application of anti-virus software, appliance and software personal firewalls provide an added layer of security for machines connected to the Internet. Challenges, curiosity, and criminal intent are some of the factors of motivation that will keep attackers keen on compromising and exploiting systems. Anti-virus software provides a mechanism to detect and protect against malicious software and personal firewalls provide a mechanism for detecting and preventing malicious data packets. The computer industry is seeing changes in personal security technologies for detection and protection of malicious software. This is sparked by increased malicious software threats and the diversity and sophistication of attacks. It can be seen that the traditional security software provide valuable and adequate protection but as the threat level and sophistication increases, they will no longer be suitable for malicious software management. Amongst the many threats that exist to date, Goner proved to threaten the existence of this security software.

It is very difficult to predict the threat scenarios that will be presented in the future. What can be done to avoid these risks is ensuring that security best practices are applied that will combat these threats as they arise.

Endnotes & Bibliography

[1] " Financial losses due to Internet intrusions, trade secret theft and other cyber crimes soar." Computer Security Institute. 2001
URL: http://www.gocsi.com/prelea/000321.html (4 Jan. 2002).

[2] "VIRUSES: Preparing for the Onslaught." Information Security Magazine. May 2001.
URL: http://www.westcoast.com/securecomputing/2001_05/cover/cover.html (4 Jan. 2002).

[3] Malcolm, Andrea. "Virus Damage Estimates in 2001." Virus News Volume 7 Issue 1 (January 2002)

[4] Scambray, Joel; McClure, Stuart; Kurtz, George. Hacking Exposed, Second Edition. (Berkeley: Osborne/McGraw-Hill, 2001): 650.

[5] Graven, Mathew P. "Personal Firewalls" PC Magazine. 3 January 2001.
URL: http://www.zdnet.com/products/stories/reviews/0,4161,2669359,00.html (23 Jan.2002).

[6] Northcutt, Stephen. "Bad things that happen to good organizations!". Internet Threat Brief (2001): 4-20

"F-Secure Virus Description-Goner." F-Secure. 4 December 2001.
URL: http://www.fsecure.com/v-descs/goner.shtml (24 Jan.2002).

"W32.Goner.A@mm." Symantec Security Response. 4 December 2001.
URL: http://securityresponse.symantec.com/avcenter/venc/data/w32.goner.a@mm.html (24 Jan.2002).

Wack, John. "Guidelines on Firewalls and Firewall Policy." Information Technology Laboratory Bulletin. January 2002.
URL: http://csrc.nist.gov/publications/nistbul/01-02.pdf (24 Jan.2002).

"Firewall Technologies." Carrier IP Information Exchange. 2001.
URL: http://www.cipx.net/subjects/firewalls.htm (6 Feb. 2002).

"Netscreen-5XP Robust easy-to-use management." NetScreen. 2001.
URL: http://www.netscreen.com/products/appliances.html#ns5xp (13 Feb.2002).

"RapidStream 500 High-Performance Telecommuter VPN/Firewall Security Appliance." RapidStream. 2001.
URL: http://www.rapidstream.com/pdfs/RS500_datasheet.pdf (13 Feb.2002).

"The Ultimate Packer for executables." UPX Homepage. 23 May 2001.
URL: http://upx.sourceforge.net/ (14 Mar. 2002).

Nachenberg, Carey. "Behavior Blocking: The Next Step in Anti-Virus Protection." SecurityFocus. 19 March 2002.
URL: http://online.securityfocus.com/infocus/1557 (21 Mar. 2002).

Last Updated: July 26th, 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