Global Information Assurance Certification Paper

I Know What Your Browser Did Last Night

An Analysis of Brower Helper Applications and Security

Ronald L Ropp
GIAC Security Essentials Certification (GSEC)
(February 2004)
Practical Assignment Version 1.4b Option 1

Abstract

This paper studies the issues and security implications surrounding many popular “helper applications” and BHO’s (Browser Helper Objects). We will begin by a brief background and a line up of the “usual suspects” that fit into the helper application categories and how they are typically found, installed or otherwise “plugged” into our computer systems.

We will then move on to briefly analyze basic network traffic generated by “normal” systems and compare that to systems with these applications running and analyze the security and privacy implications. The scope of this paper is really to create awareness of client initiated communications and the security implications it can have. We will then cover several methods to detect, clean and analyze these applications using several readily available tools at little or no cost.

Introduction

Communications and the Internet, and the applications that use it continue to evolve and change. Users continue to want more functionality and ease of use, and many advances have been made in the area of rich communication and intuitive interfaces. Web browsers and other applications continue to become more interactive with this medium, and not simply a “viewer” of the information presented. Users want ease of use and instant information regarding their areas of interest. Today we especially see this in the always-on broadband Internet home, and corporate networks.

With the demand for interactivity, came the functionality from the static online web pages to more dynamic specific content, and tailored delivery. Major vendors started to support “active” content with programming languages like Java, Javascript, etc. The online content then started to become a more viable “mainstream” medium not just confined to the propeller heads that inhabited the space. Advertising and data collection on user habits, and driving traffic to web sites supposedly translated to more revenue.

Companies and less savory characters started creating ways to capture users habits and places they went. This provided ways to push dynamic content based upon the user via banners ads, pop-up’s and other means. The most common method of course was cookies, but soon this was not good enough and more detailed ways of doing this became available. The trick was they needed a way to get that “helper” program installed on the client system so they could really get the keys to the car. By getting these programs installed (which will be demonstrated later in this paper) companies and the bad guys are able to on many occasions get by the security mechanisms in place in most enterprises or home systems. The most obvious reason is that on many occasions the

communication is initiated by the client, or via HTTP traffic that may not be monitored or filtered as closely (or at all) at home or in a corporate setting.

If these programs were simply confined as Spyware:(A general term for a program that surreptitiously monitors your actions.[1]) and did nothing more, then it might simply be an annoyance and something that the privacy advocates would continue to fight. Unfortunately many of these programs can do much more harm, and pave the way for identity theft, fraud, and system compromise.

The Line Up

There are far to many to list within the context of this paper, however it would be beneficial to outline some definitions as recognized for the ever-growing family of these applications. After we go over these basic definitions we will recognize a few of the most popular and effective applications that seem to be omnipresent today.

Definition guide of popular terms:

1. **A Browser Helper Object or BHO,** is just a small program that runs automatically every time you start your Internet browser. Usually, a BHO is installed on your system by another software program. For example, Go!Zilla, the downloading utility, used to install a BHO created by Radiate (formerly Aureate Media); this BHO tracks which advertisements you see as you surf the Web. [2]
2. **Adware**, also known as an Adbot, can do a number of things from profile your online surfing and spending habits to popping up annoying ad windows as you surf. In some cases Adware has been bundled (i.e. peer-to-peer file swapping products) with other software without the user's knowledge or slipped in the fine print of a EULA (End User License Agreement).[2]
3. **Cookie**, a packet of information sent by a server to a web browser and then sent back by the browser each time it accesses that server Cookies can contain any arbitrary information the server chooses and are used to maintain state between otherwise stateless HTTP transactions. Typically this is used to authenticate or identify a registered user of a web site without requiring them to sign in again every time they access that site, and tracking a particular user's access to a site.[3]
4. **Spyware** is computer software that aids in gathering information about a person or organization without their knowledge. The most common use of spyware is to gather information about the user and relay it to advertisers or other interested parties. It has also been used by law enforcement to collect evidence against criminal suspects[3]
5. **Malware** (a contraction of "malicious software") refers to software developed for the purpose of doing harm. [3]

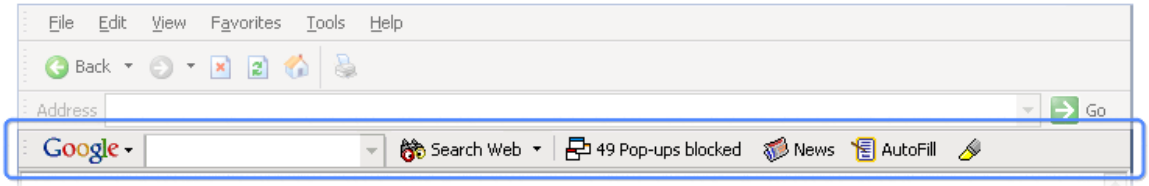
There are a plethora of other terms and jargon related this topic, and is beyond the scope of this document.
It quickly becomes apparent that there are several programs and definitions that blur the lines. This is less important however than the point that these programs exist and are very clever in the many ways they can get themselves installed on the unwitting target. Most of them have one thing in common however, in that they rely on some end user action (in most cases) to install and run.

Many people on both sides of the fence argue by definition that software that is installed voluntarily by an end user is valid software that is not classified as spyware, or other "unsolicited commercial software". This software on many occasions provides a utility that the user primarily desires and buries consent to monitoring or other functions with a lengthy end user agreement that most people do not bother to read, or cannot understand the complex legal wording. Other programs by nature may install "optional" components that the average end user may not be aware are being added as part of a "normal" install.

Below is a listing of typical methods that entice the average user.

1. **Toolbars or web search bars** – These convenient BHO's add functionality typically to Microsoft's Internet explorer and will add additional rows of buttons to do things like quick searches, block pop up ads, or even give you email alerts, etc. Again the usage by some popular providers seems perfectly legitimate and functional. There is safety in numbers however, and careful selection and analysis (including reading the fine print) is needed. There are many very invasive and difficult to remove versions that exist as well.

(Example of popular google browser toolbar)(4)

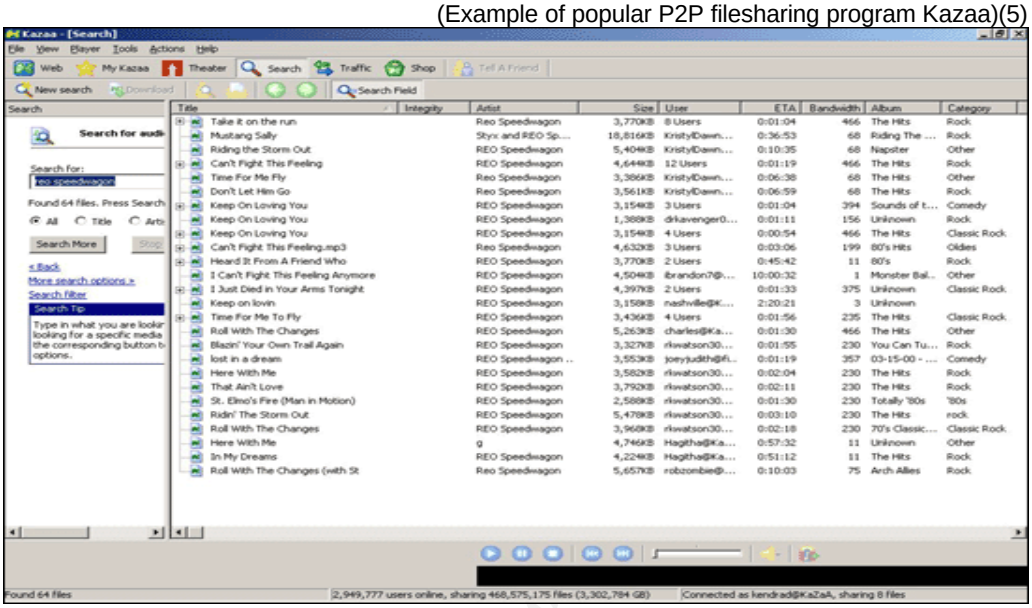


2. **P2P (peer to peer) file sharing programs** – These programs are enormously popular for people to share files for a variety of reasons, and have received plenty of press from the media and the RIAA fight associated with illegal music downloads. Music is not item of value on these networks, and they attract all types of information, programs, etc. Not only are many of the files on these networks infected with viruses, Trojans, etc. The programs themselves typically share a folder on your

local hard drive, and in some cases the program itself will perform malicious activity (or at least risky) on your system.

P2P – Cont.

(Example of popular P2P filesharing program Kazaa)(5)



3. **Web Companions and utilities** – These are a variety of handy programs that might perform mundane tasks that make your online life a little easier. Typical applications are things like weather information, remembering info and filling out forms for you, remembering passwords, stock quotes, reminders, or even animated characters. Many of these programs fall right into the borderline category and require close analysis as they do many of the same things that other programs listed previously do like tracking activity, pop up ads, and more.

BONZI.COM – Example of Bonzi Buddy(6)

These are just broad classifications of types programs, and there are numerous others that fall in and out of all three of these areas. There are new and different ways that clever advertisers and malicious folks are finding to gain information and access to your systems daily. But in most cases these applications however installed typically require some sort of end user action. (ie. Execution of code,).

Analysis Example

To gain a better understanding of what is happening when these types of programs are running, we are going to take a short look at differences in communications between a machine that is not running any of the above type of programs, and then what that communication looks like after tools like the ones above are installed. The basic layout will be as follows.

A. clean machine browsing a web site
B. machine running a BHO or utility as listed above surfing the same site
C. Implications and analysis of what it means

We will not get into tools for detection and how to clean these types of programs in this section, as it will be covered in the next section.

Case #1a – Clean Windows XP machine running Internet Explorer 6.0 (simply starting up browser and going to www.internetcds.com) Below is an initial capture of the traffic between the client and the web site.

Source	Destination	Protocol	Info
192.168.1.2	206.xxx.xxx.xxx	DNS	Standard query A www.internetcds.com
206.xxx.xxx.xxx	192.168.1.2	DNS	Standard query response A 63.xxx.xxx.xxx
192.168.1.2	63.xxx.xxx.xxx	TCP	1314 > http [SYN] Seq=1698109515 Ack=0 Win=65268
63.xxx.xxx.xxx	192.168.1.2	TCP	http > 1314 [SYN, ACK] Seq=1097874495 Ack=1698109516
192.168.1.2	63.xxx.xxx.xxx	TCP	1314 > http [ACK] Seq=1698109516 Ack=1097874496
192.168.1.2	63.xxx.xxx.xxx	HTTP	GET / HTTP/1.1
63.xxx.xxx.xxx	192.168.1.2	HTTP	HTTP/1.1 200 OK
63.xxx.xxx.xxx	192.168.1.2	HTTP	Continuation

As illustrated above, the client (192.168.1.2) requests the domain name typed into the browser of www.internetcds.com the DNS server responds with that IP address, and the client then initiates the standard three step handshake with the web server (63.xxx.xxx.xxx) and standard HTTP communications commence.

Case #1b – Windows 2000 machine running popular BHO that adds a toolbar to the browser as illustrated below. This could be added via a website, or email inviting a user to get cool new tools for their browser.

The communications between the client browser (192.168.1.5) and the web site (208.xxx.xxx.xxx) it is trying to access starts out normally.

Source	Destination	Protocol	Info
192.168.1.5	206.xxx.xxx.xxx	DNS	Standard query A www.convergecomm.com
206.xxx.xxx.xxx	192.168.1.5	DNS	Standard query response A 208.xxx.xxx.xxx
192.168.1.5	208.xxx.xxx.xxx	TCP	1095 > http [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=1460
208.xxx.xxx.xxx	192.168.1.5	TCP	http > 1095 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0
192.168.1.5	208.xxx.xxx.xxx	TCP	1095 > http [ACK] Seq=1 Ack=1 Win=17520 Len=0
192.168.1.5	208.xxx.xxx.xxx	HTTP	GET / HTTP/1.1
208.xxx.xxx.xxx	192.168.1.5	HTTP	HTTP/1.1 200 Ok

But suddenly the client (192.168.1.5) begins talking to someone else (165.xxx.xxx.xxx)!

Source	Destination	Protocol	Info
192.168.1.5	165.xxx.xxx.xxx	TCP	1096 > http [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=1460
165.xxx.xxx.xxx	192.168.1.5	TCP	http > 1096 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0
192.168.1.5	165.xxx.xxx.xxx	TCP	1096 > http [ACK] Seq=1 Ack=1 Win=17520 Len=0
192.168.1.5	165.xxx.xxx.xxx	HTTP	GET /dynamic/hotbar/disp/3.0/sitedisp.dll?GetSDF&Dom=convergecomm.com&Path=%2f&SiteVer=0 HTTP/1.1
165.xxx.xxx.xxx	192.168.1.5	HTTP	HTTP/1.1 200 OK
165.xxx.xxx.xxx	192.168.1.5	HTTP	Continuation

1c. Implications and what this means

Basic web browsing is something most people do at work or at home almost daily. It has become an invaluable tool in many areas. Most corporate networks and home systems are built around this, and are built around keeping the bad guys out of your network. There is however a critical component to understand about client initiated communications and the implications that programs have that end users may run that create security holes directly or indirectly to your home or corporate network.

In the above example with the computer running the toolbar program (BHO-malicious or not), the end user installed a program that appears to be sending info about what web sites I am going to (www.convergecomm.com) to someone else. (That I do not know, and did not ask to go to).

192.168.1.5	165.xxx.xxx.xxx	HTTP	GET /dynamic/hotbar/disp/3.0/sitedisp.dll?GetSDF&Dom=convergecomm.com&Path=%2f&SiteVer=0 HTTP/1.1

However upon deeper inspection I found something much more troubling by looking into the packets that delivers the information between my computer and this stranger.

```
GET /dynamic/hotbar/disp/3.0/sitedisp.dll?GetSDF&Dom=convergecomm.com&Path=%2f&SiteVer=0 HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 5.01; Hotbar 4.4.2.0)
Host: abccompany.toolbarthatisinstalled.com
Connection: Keep-Alive
Cookie: ui=009CE6E075E6A0489DD5D3B31DCD47B0271CCB84;
ci=F4DE65B972E04E4D89594844FE712609B605A7C3; Partner=hotbar; create_date=02/19/2004 07:29:26;
User=password=qhrg05&UserName=biff%40ibiff%2Ecom&LoggedIn=yes; sg=sg506; country=US;
SDCU=111E780002371
```

My computer is sending information to this stranger about me (initiated by me!). My location, user name, password !, and email address. While this information might simply be my user information to access this particular toolbar program or it's associated web site services, it is clearly insecure (HTTP traffic in clear text).

Now the human factor coupled with this information starts to gain strength in possible security breach of your own systems. Why?

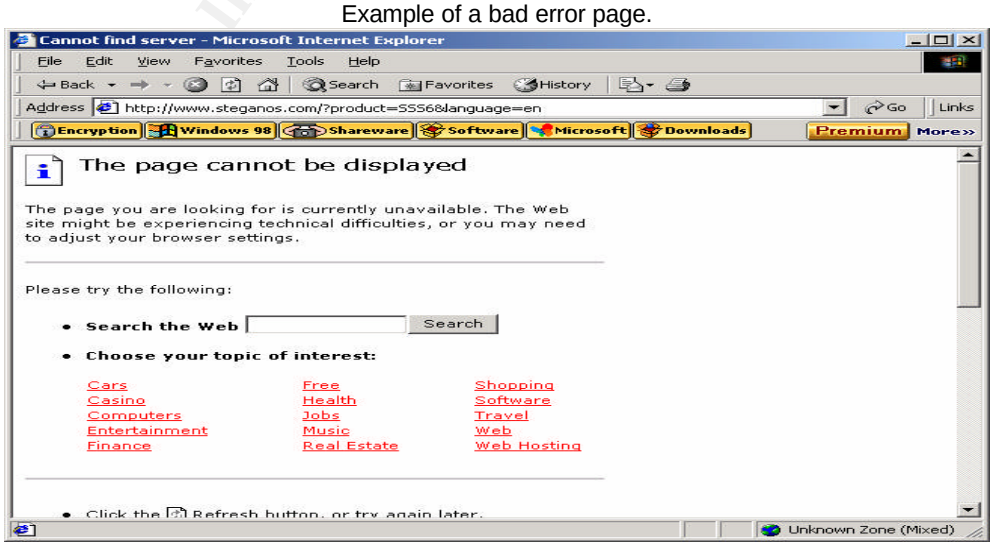
Scenario: End user signs up and uses this toolbar and service innocently enough on their computer and advertisers collect data, and everyone is happy. However your HTTP outbound traffic is simply motoring along in clear text to the outside world. Now what would most end users do when setting up a new account when queried to enroll with a user name and password?

We have to many passwords to remember already, so we use the few that we can remember over and over, or for the sake of simplicity the end user uses his or her same password and email for at home or on the corporate LAN for "convenience". As you can see then you would have a huge issue with a seemingly innocent "utility" program. This is why many hackers do not attack or break down walls to gain network access, when they can simply sit back and watch the traffic go by and pick up data that might quickly give them intelligence to walk right through the front door.

A couple more basic indicators that you may have some sort of software running on your browser that is doing a bit more than you are aware or want it to, is strange results from searches or when you start your browser the home page is changed to something undesirable. You change it back manually, but before too long you find it has changed back again.(7)

Also your Internet error pages may have some strange messages or search options.

Example of a bad error page.



This basic analysis is just one example of one BHO that could potentially lead to serious security risks. There are hundreds (if not thousands) of other types of programs like these that integrate with your Web browser. Not to mention the other utility type programs and P2P file sharing programs mentioned briefly above.

There are two basic things to keep in mind when considering the use, audit and defense of this type of software.

1. What are my end users installing on their computers (or what am I installing on my computer), and is the source trusted? Even if it is trusted, what type of behavior does it exhibit while using it online.
2. How do I look at, filter, or monitor client initiated communications from a security perspective?

The good news is that there are many good tools to watch, clean and protect systems from these types of hazards.

Tools to Use

The tools used in this category generally fall into two basic areas.

- Detection and removal
- Active or ongoing monitoring

We are going to take a brief look at one well-known tool used primarily for detection and removal of the programs.

Detection

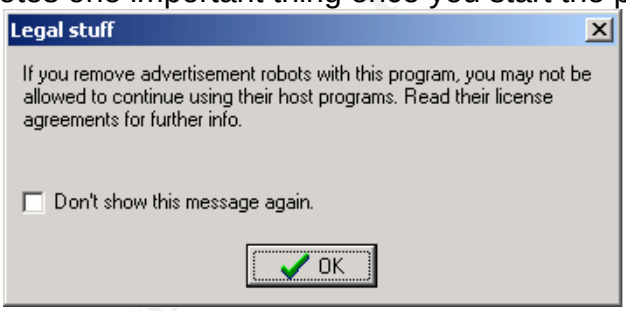
There are many good tools that exist that are readily available on the web and can come as shareware, freeware, or corporate editions that will perform many of the same functions. While we are only addressing the detection primarily of Spyware, BHO's, etc. not virus protection, many of these programs will detect Trojans and other malicious programs, but are not a replacement for virus protection, just a compliment to an overall security strategy.

Many names of these programs that come to mind can be found and reviewed on CNET[8], and many other locations.

The program that we will take a quick look at is Spybot Search and Destroy by PepiMK Software[9]. To quote CNET's review. "For protection against ad-serving software, Trojan Horses, and other means of tracking your surfing habits, get Spybot immediately." [10] This is not an endorsement by using this as our example, just one tool in many that you can research and find that are very inexpensive (or free in this case).

After installation, the screen and interface is quite easy to understand and use.

It also notes one important thing once you start the program.



Many programs use the advertisement or spyware type functions included as the gatekeeper to the program actually working. So you must be aware that using programs like these and removing the registry keys, etc. Could very likely disable the main functionality of a particular program that you actually want. As stated above, you should read the license agreements for the software you are installing.

After a quick scan of the system that the toolbar was installed on, the program found 64 instances of the toolbar program strewn about the system. Many of these instances were registry entries and make the program quite embedded within your operating system. This of course makes in difficult to un-install. This particular toolbar actually had an un-installer available in the control panel add-remove option in Windows. Many of them do not have any removal option available.

Even if they do have a removal option, a scan after uninstall is recommended to see if any remnants remain. Another scan on our test system revealed that after

we used the windows uninstaller that 1 file still remained, that was then deleted to be sure that the system was completely clean. As stated earlier, many programs do not have an uninstaller, and you have to resort to a manual extraction or search online to find out how to remove the programs. There are several good web sites dedicated to this process, and several of the major vendors also provide help for some in this area.

One interesting note that most people ask is, Why doesn't my anti-virus software detect this? Below is the best explanation that I have found from a popular web site.(11)

> Technically, most unsolicited commercial software isn't viral: it doesn't spread from computer to computer, it just installs and runs on one system.
>
> That doesn't mean it's not harmful, but anti-virus software does not attempt to detect all software that could be harmful. Whether it *should* is a tricky argument that ends up a question of where you draw the line.
>
> Actually some anti-virus programs do detect *some* of the parasites outlined on these pages, but not nearly all, and not all versions of them. Parasites that install using IE security holes are more likely to be targeted by the anti-virus software vendors, but the selection of targets seems for the most part to be pretty arbitrary.
>
> For this reason there are now a number of anti-parasite packages around that work as a complement to anti-virus software.

Again reinforcing the notion that a layered approach to your security is the best approach.

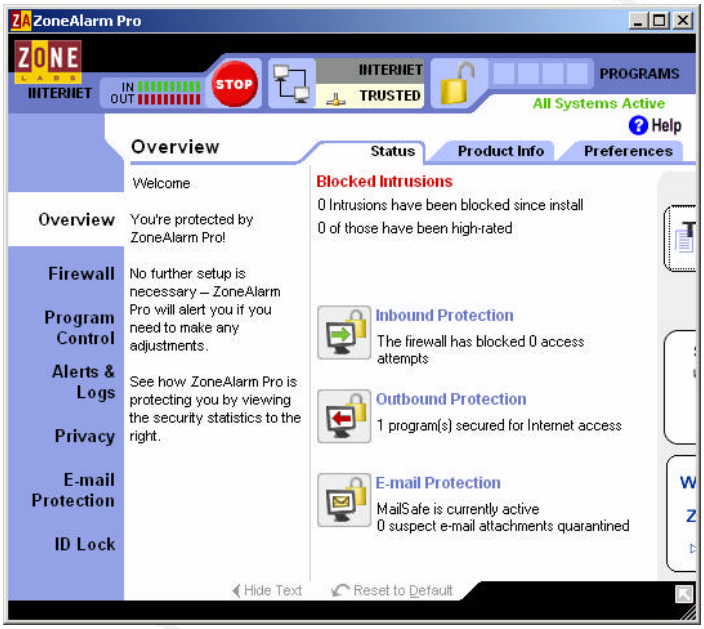
The next category of tools is ongoing real-time monitoring tools. There are several that are available that may fall into the category of intrusion detection like Snort(12) or even enterprise software that would inspect incoming and outgoing traffic. Keeping the desktop theme, we are going to look briefly at a desktop application firewall called Zone Alarm (13) by Zone Labs. It has several different versions you can choose from, including a free one. We are not going to get into all of the details that encompass different types of firewalls, and how to exactly configure all of the options. That could be another entire paper writing the intricacies of that type of work.

The basics of Zone Alarm is that it is a firewall that will monitor all programs on your desktop that try to access the internet and will prompt the user to decide whether or not you want to grant a particular level of access to the application in question (just one function of this program that will do many other things as well),

that you may not have known was accessing the Internet until you installed this program.

The Zone Alarm installation is your basic windows install and you can follow the prompts and even the wizards in a default install and it will provide a good measure of security. (It is recommended however to spend some extra time to learn and configure the program specific to your environment and applications to ensure the greatest level of security.)

The basic interface allows for a granular level of control over many attributes of your connectivity.



After install it was only about 2 minutes when the computer with the browser toolbar program reinstalled to get the following prompt.

A program called HbSrv was trying to access the Internet to an IP address that was not put into my browser for surfing purposes, or accessed from my email client. Since the program was unfamiliar to me, and I did not launch it, I can decide whether or not to block that program from accessing the Internet. I can also tell Zone Alarm to remember whether or not I want to it to ask me every time it happens, or remember my decision.

Of course this again is only a measure of control and security because we are leaving the decision up to the end user (or yourself) to decide whether or not this program is trusted or not, but it is certainly a step further than we were prior to installation, when we did not even know that this program was running and accessing the Internet from my computer. Zone Alarm will run in the background and keep and eye on all incoming and outgoing communications and applications real time, which will help prevent the human habit of procrastinating or remembering to perform scans in a timely fashion. Which is the one major difference between real time and user-initiated programs that protect your system that may be connected real time to the Internet at all times.

Conclusion

Connecting to the Internet and not being aware of who your computer is talking to can be hazardous to your computers health. The additional functionality and interaction that we all crave can come at a price, and a system or network compromise might occur if we do not practice a measure of caution. A well-planned security approach to all of your network traffic, including client initiated traffic over channels that may be considered safe, or utilitarian in nature (ie. HTTP) is important. The end users or casual home user must have guidelines and understand what things to watch for and to help participate in the security process.

Installing software of any type on a system can introduce security risks, even when they may be un-intended by the vendor who is trying to simply gather statistics. Also without standards or awareness of how the application may behave on the network or desktop can even disable to break other security mechanisms that may be in place. Sending information about users, email addresses, passwords, etc. when unknown by the user and in clear text is a prime candidate to be collected remotely by others who are building intelligence about you, your network, and how to execute a compromise.

The bad guys are numerous, but so are the tools and the community that helps develop the protection to combat them.

References:

1. Internet Security Systems – Black Ice Glossary
   http://blackice.iss.net/glossary.php (Last accessed February 2004)

2. Spywareguide.com – Terms and Definitions
   http://www.spywareguide.com/term_list.php (last accessed February 2004)

3. Wikipedia – The free enyclopedia – Spyware
   http://en.wikipedia.org/wiki/Spyware (last accessed February 2004)

4. Google – Google Toolbar
   http://toolbar.google.com (last accessed February 2004)

5. CNET Networks Inc.– CNET reviews – "Kazaa 2.0", September 24th, 2002
   http://reviews.cnet.com/Kazaa_2_0/4505-3513_7-20456501.html?tag=dir
   (Last accessed February 2004)

6. Bonzi Software Inc. – New! BONZI Buddy!
   http://www.bonzi.com/bonzibuddy/bonzibuddyfreehom.asp
   (last accessed February 2004)

7. Rubenking, Neil J. "11 signs of Spyware"
   PC Magazine March 2, 2004 (2004) pg. 87

8. CNET Networks Inc, CNET reviews from CNET Labs
   http://reviews.cnet.com (last accessed February 2004)

9. PepiMK Softare – Spybot Search and Destroy
   http://spybot.safer-networking.de/index.php?page=home
   (last accessed February 2004)

10. CNET Networks Inc., CNET review – "Spybot Search and Destroy"
    http://reviews.cnet.com/Spybot_Search_and_Destroy/4505-3514_7-20848563.html?tag=dir
    (last accessed February 2004)

11. Andrew Clover – and.doxdesk.com – "What are Parasites?"
    http://217.115.153.73/parasite/ (last accessed February 2004)

12. Sourcefire Inc. Snort.org – The open source intrusion detection system
    http://www.snort.org/team.html (last accessed February 2004)

13. Zone Labs Inc. – Internet Security Products
    http://www.zonelabs.com/store/content/home.jsp (last accessed February 2004)