GIAC
CERTIFICATIONS

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 (Security 401)"
at http://www.giac.org/registration/gsec

NetBus 2.1, is it still a Trojan horse or an actual valid remote control administration tool?

By Seth Kulakow

Date: 2001/08/21
Revision: 1.2f

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Table of Contents

INTRODUCTION

3

NETBUS 2.1

4

CASE STUDY

10

CONCLUSION

13

FOR FURTHER INFORMATION

13

REFERENCES

14

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Figures

Figure 1: McAfee Virus Map

4

Figure 2: Past NetBus Icons

5

Figure 3: Screen Shot NetBus 1.7

5

Figure 4: Screen Shot NetBus 2.1 w/Toolbars

6

Figure 5: Screen Shot NetBus 2.1 w/Host Options

7

Figure 6: Screen Shot Control Options\Server Admin

7

Figure 7: Screen Shot NetBus 2.1 Control Options\File actions

8

Figure 8: Screen Shot NetBus 2.1 Control Options\Spy Functions

8

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Figure 9: Screen Shot NetBus 2.1 Control Options\Exit Window Options

9

Figure 10: Screen Shot Control Options\Cool functions

9

Figure 11: Screen Shot Windows 98 Registry NetBus 2.1

12

Figure 12: ZDNet Security Downloads

14

INTRODUCTION

The term Trojan has been around for hundreds of years. While it originally meant a warrior from the City of Troy, because of Homer's *Iliad,* it has come to be used to describe one thing hidden by a larger less threatening object. This term has had resounding success from day one. The Greeks used it to gain access to the City of Troy, a fortress city. Unfortunately, times really haven't changed that much. From Homer's *Iliad*, "during the night the warriors emerged from the wooden horse and overran the city". Today, you wouldn't have a very large wooden horse around your computer(s). One would almost certainly sense a potential situation right away. A 30' tall horse usually stands out from the daily norm. However, the Trojan concept is very much alive and active throughout the computer world.

Let's delve into the topic of Trojans, specifically NetBus 2.1. Now, NetBus 2.1 has really intrigued me since I finished the Kickstart and GSEC classes in Denver 2001. For those who might be reading this paper and finished the Kickstart and GSEC classes and would like to know about the location of the classes' discussion on NetBus 2.1, please refer to the K.3 book Intrusion Detection *The Big Picture-Part II* page 2-55 Infection with NetBus.

To start this journey, let's first define what the computer world's definition of a Trojan is. The American Heritage Collage dictionary 3rd edition defines a Trojan as "a person of courageous determination or energy". It also defines a Trojan horse as "a subversive group or device placed within the enemy ranks". Another definition from searchsecurity.com defines a Trojan horse as "a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can control and do its chosen form of damage". Combining all definitions together makes a determined person or group that considers you the enemy and more

© SANS Institute 2000 - 2005 Author retains full rights.

than likely has malicious intentions.

In any form, Trojan horses are meant to do an assortment of remote control access. From complete computer control such as file uploading, downloading, and deleting to password cracking, distributed denial of service attacks (DDOS), backdoor creation, etc. Trojan horses are sometimes vicious in nature, can be hard to detect and very hard to remove, once infected (A virus is a malicious program that is intended to corrupt or destroy data). Security personal must be prepared for old, present and new Trojan horse threats everyday. Otherwise they risk having their environment grind to a halt. Thus, potentially losing valuable information and causing potentially significant recovery time, to say the least. According to McAfee.com (see figure 1 below) in the last 30 days 32.41% of all computers using McAfee virus protection had some form of virus infection.

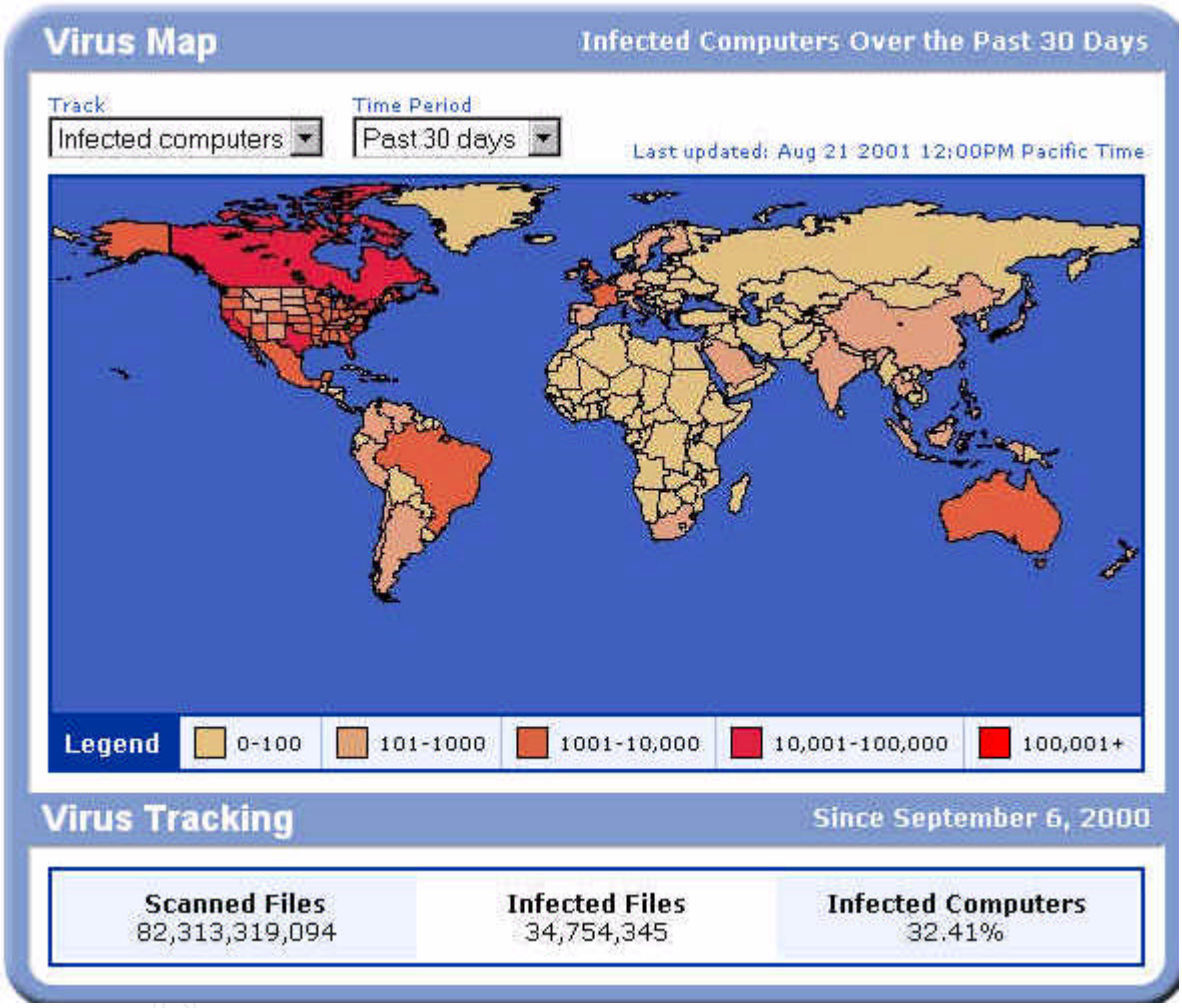


Figure 1: McAfee Virus Map

McAfee and Norton virus detection programs consider Trojan horses as virus infections. Now this is by no means implying that all the infected computers were Trojan horses viruses. However, it would be safe to say that decent percentages are. In addition, the current code red bugs propagating around could be padding the infected computer numbers. Anyway, NetBus v 1.2 – 1.7 are considered Trojan horses and detectable by McAfee, Norton and other various detection software.

© SANS Institute 2000 - 2005 Author retains full rights.

NETBUS 2.1

Lets finally get back to what this paper is intended to explain, NetBus 2.1. A Swedish programmer named Carl-Fredrik Neikter developed NetBus around early 1998. Version 1.2 started out solely as a Trojan horse program intended to go out and gain remote control over a person's computer. V1.2 was soon displaced by version 1.5 with the same intensions as V1.2. As with most new code releases, it provided new features and fixed old problems. Now around the same time V1.5 was released, Back Orifice hit the Internet. The media hype and problems it created really started the fast evolution of Trojan horse development to what it is today. As virus detection products began to detect a version of NetBus, a new one was then developed. V1.5x was displaced by V1.6 and then to V1.7. Each version of NetBus had an executable sent along with it. All the user would do is double click on an icon or attachment (see figure 2 below) and the Trojan horse was off and running in the background without the users knowledge. Also, all icons could be interchanged to anything an attacker wanted by using simple icon software (internet freeware). The following are the standard attachments for the Trojan versions of NetBus.



2: Past NetBus Icons

In addition to the .exe placed in an email to someone saying, something like, click on this patch to fix a certain problem. It could even be placed into a game such as Whack-a-mole or Game.exe. When you started the game you started the Trojan horse. Below is a screen shot on what an attacker could do to an infected computer using V1.7.

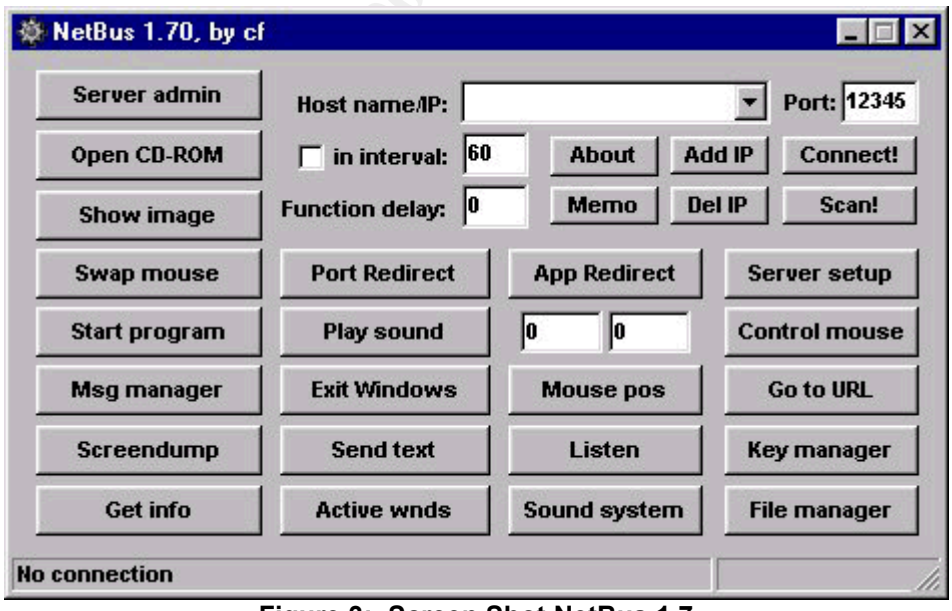


Figure 3: Screen Shot NetBus 1.7

It's scary to think that someone could not only listen to you through your computer, but do just about anything nasty they wanted, like email the Trojan horse to others in your network using your email address.

Fortunately for the security community, virus scanners and other means like netstat

© SANS Institute 2000 - 2005 Author retains full rights.

commands can detect NetBus 1.2–1.7 (we'll get to netstat later). Even more fortunate is the fact that NetBus 2.0 and 2.1 are meant to be legitimate friendly software (I do say this with much jest). Yes, that is right. Carl-Fredrik Neikter says that he doesn't want it used as an attack tool anymore and it should be used as a legit remote admin tool. However if you didn't already figure it out, it is still a very nice tool to use for the other purpose. Before we go through what it has, let me first say that it is easy to install. One must realize that the attacker is the client and the victim's computer is the server. Once you install the client on your machine and install the server on someone's computer (which can run invisible), then you scan for that server and it should show up connected. Now, I won't go into any more detail on install and set up just because if I can do it with relative ease, than most people can. So try it on your own. But get permission first from the people you plan on infecting before you start remotely administering their system.

NetBus 2.1 looks like the following screen captures (see figures 4 – 10 below). A lot of new features have been added since V1.7. It has a nice GUI interface and easy pull down menus and to make it really legitimate advertisements. One "necessary " remote administration tool is you can now view, if the computer has one, their net cam. The trend in the computer desk and lap top business is to provide ever-growing pre-configured standard system features such as net cams. Call it the new "big brother" but by your own cam this time. Other features include:

- Easier use of keyboard logging
- Screen dumping
- IP range scanning for other servers
- Scripting
- Broadcast sending for host command broadcasting
- Registry management
- Windows manager for window control
- Plugin manager for new plugins
- File manager which allows full control of the users files
- Etc.

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

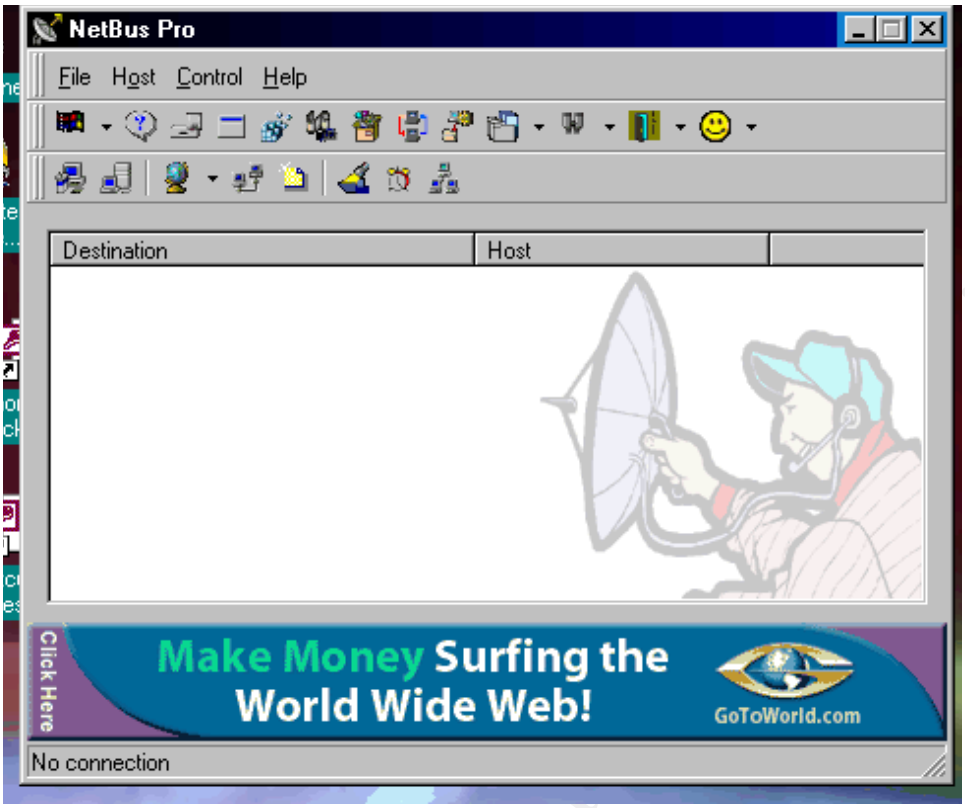


Figure 4: Screen Shot NetBus 2.1 w/Toolbars

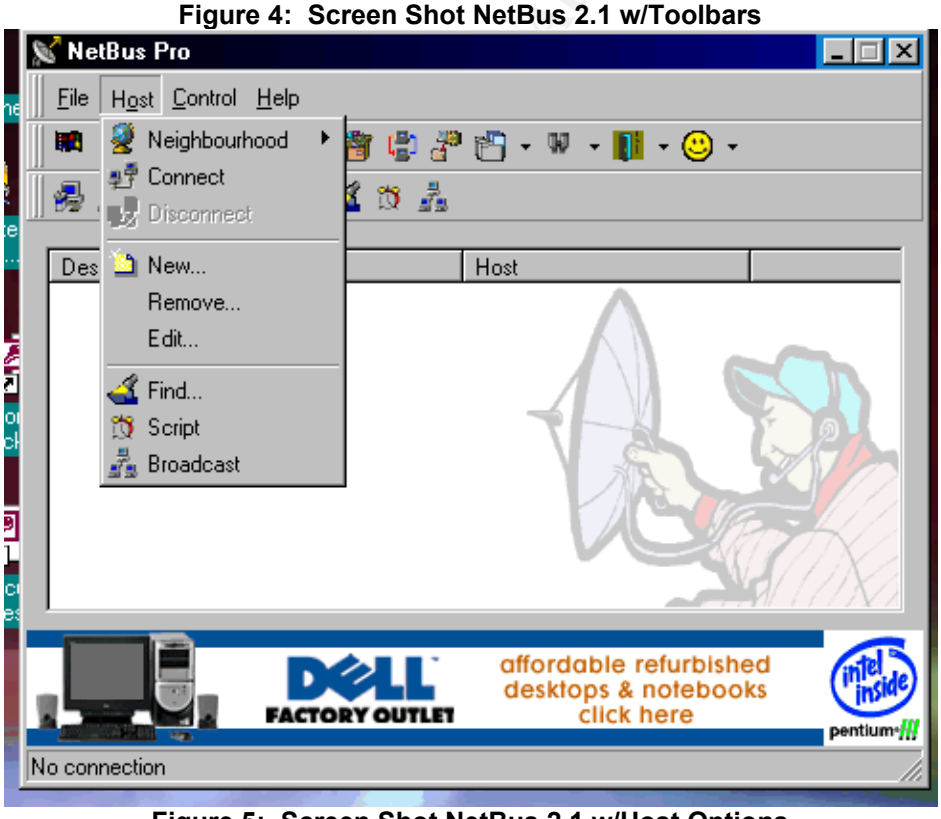


Figure 5: Screen Shot NetBus 2.1 w/Host Options

© SANS Institute 2000 - 2005 Author retains full rights.

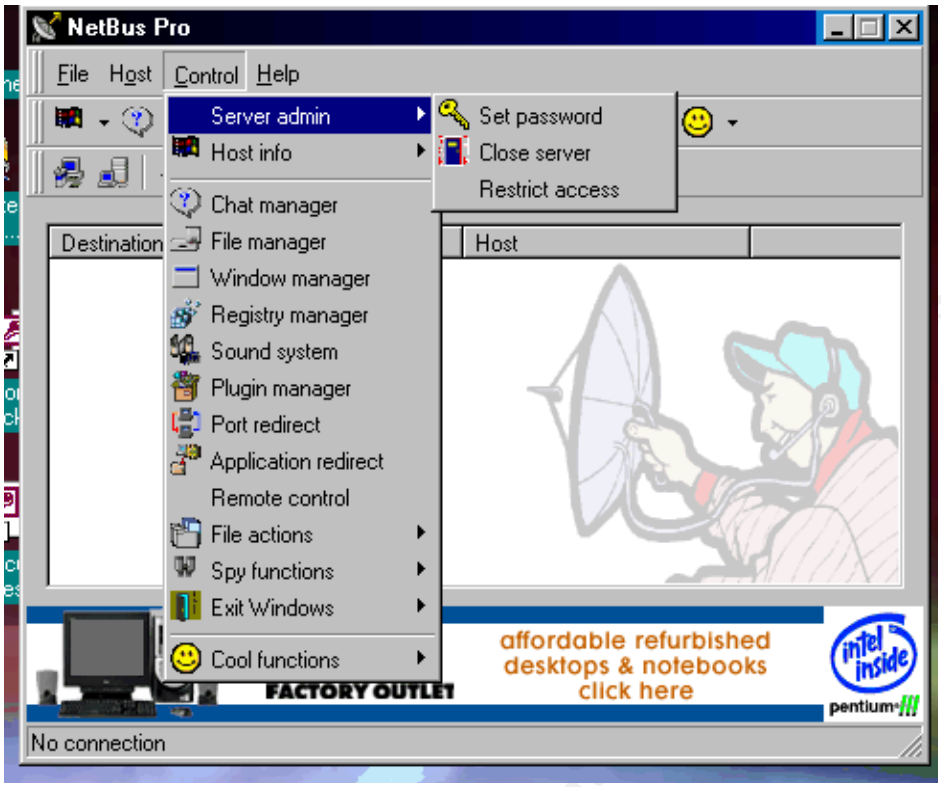


Figure 6: Screen Shot Control Options\Server Admin

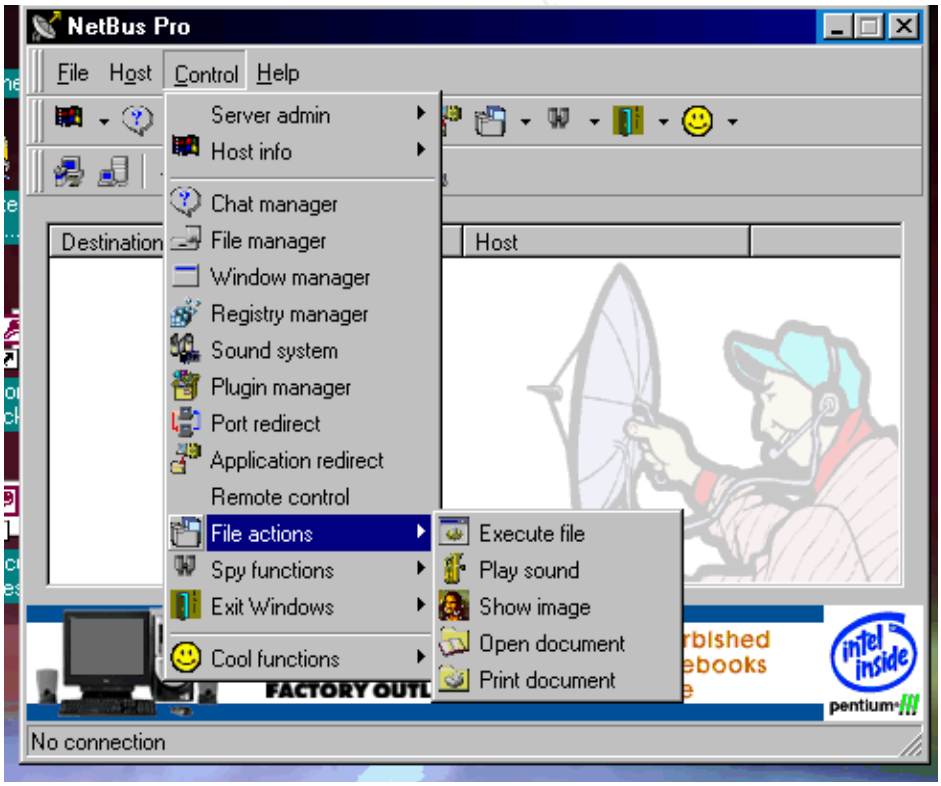


Figure 7: Screen Shot NetBus 2.1 Control Options\File actions

© SANS Institute 2000 - 2005 Author retains full rights.

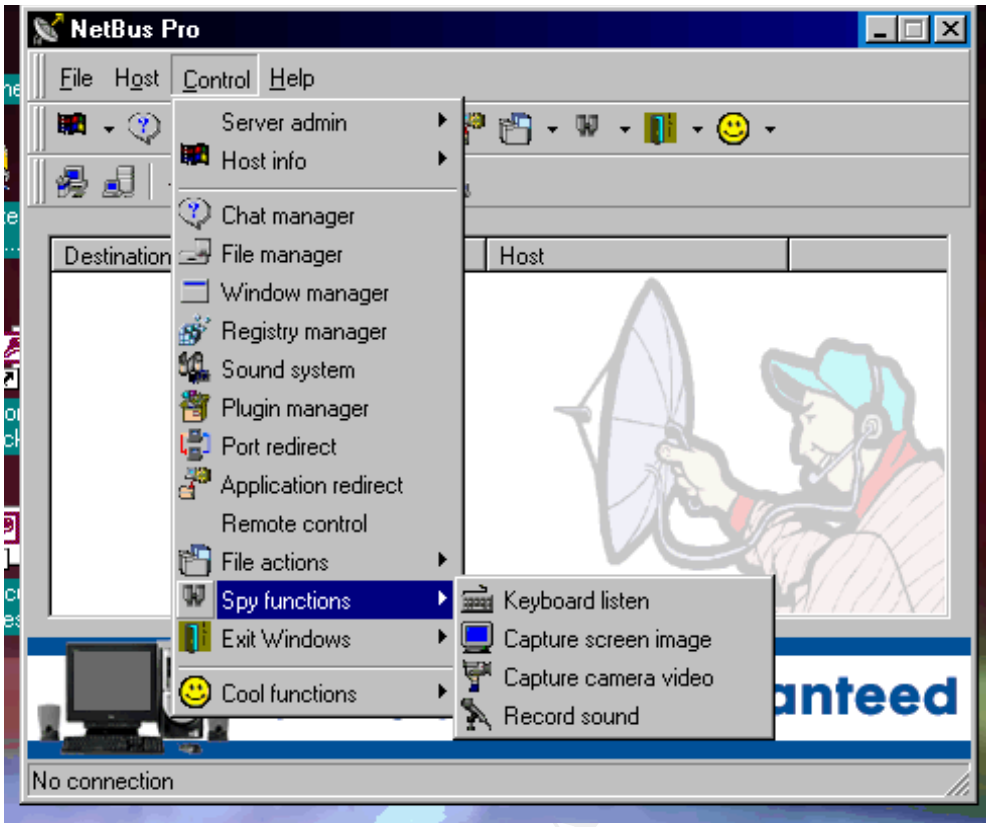


Figure 8: Screen Shot NetBus 2.1 Control Options\Spy Functions



Figure 9: Screen Shot NetBus 2.1 Control Options\Exit Window Options

© SANS Institute 2000 - 2005 Author retains full rights.



Figure 10: Screen Shot Control Options\Cool functions

It has great tools for remote administration. But how much of it is really needed for remote administration? I am not sure. For example, it's nice that you can actually check for other server computers by scanning IP ranges, which I did do on my own network to no avail. It will tell you if you have any other computers with the NetBus server installed. I already know where all my remote administration tools are placed on my network; I placed them there. I don't have to scan for them. Scanning and finding a server that you might have not placed is metaphoric to getting an invitation to a large gala by mistake but still going because it would be great time and probably no one would even notice that you were there.

There are many new features I mentioned with NetBus 2.1. However when the program was created as a Trojan horse, those same features still exist in v 2.1. I feel that this creates a cloudy line between Trojan horse and legitimate administration tool.

CASE STUDY

Lets get into the threat of this "remote administration tool" a little more. As defined by CERT 1993, a threat is "any circumstances or event that has the potential to cause harm to a system or network". So any existing or unknown vulnerabilities are system or network threats. Take some time if you haven't already to look above at the screen shots from NetBus 2.1 (funny how the main screen shows a person trying to listen in on remote conversions). All it takes is one infected system located in any part of your network to take control over almost everything company wide in a short period of time. I tested this theory. I loaded an undetected NetBus 2.1 server onto a laptop computer at our site (the start of an **internal** hack attack). Lets say that this "portable" computer travels frequently to many locations within our company. In turn, many different department network domains and VLAN's such as finance, operations, transportation, etc are exposed. Every time I powered up the server computer and connected to our network, I could see every device within that domain through NetBus 2.1's client neighborhood view, just like network neighborhood (figure 5). I now knew what users, servers, domains, etc existed; thus I could start attempts to cracking into them. But that could take sometime before I got into any system that would provide me with

© SANS Institute 2000 - 2005 Author retains full rights.

enough interest or worth. And I didn't want to take the time to crack only one system and maybe get caught before I could get control over many potential prizes (I notified and received permission from all system administrators prior to my attempts to gain entry). Since I could get remote control over an NT laptop which I found openly shared, I thought the best way to propagate the server to more machines was to use this machine and their email. To do this, I remotely loaded the NetBus server on to the Laptop and hid the server service. Then, I altered NetBus 2.1's system icon using


Setup.exe to

acad.exe and sent out a group email saying "if anyone is interested in obtaining AutoCAD 2000 with an additional feature called NetBus just click on the icon and it will automatically start to load NetBus into his/her system. I took a chance thinking that 95% of our users on our networks probably hadn't any idea of what NetBus was or what it could do and the ones who did wouldn't care about the email and just delete it. In addition, I knew when the I Love You Bug hit our site users were told not to click on the attachment and they did anyway. So from past experience, there were users who would check the attachments regardless of what they were told to do. I proceeded to send out a group email to non-computer savvy departments. The email included both the acad.exe package and the package as a zipped file. This was done because I knew that our virus protection requires some attachments to be saved to the local hard drive before they can be opened. Zipped files, on the other hand, wouldn't. Users could just unzip the attachment and start the executable. So I added directions in the email that explained how to load the software. About 50% of the recipients, from different domains, responded. Finally, I scanned IP ranges for NetBus servers. Now I had enough systems compromised to keep me busy for a while. If my intentions were not honorable, I would have then opened numerous back doors for future entertainment.

Now the network had been seriously compromised and could be attacked at anytime. Since virus protection companies now consider NetBus 2.1 as a legitimate remote administration tool, virus scans would not look for NetBus 2.1. Thus, I had time to organize what, when and whom I would go after first. I selected what I thought was a machine that looked like a power user (many more programs than the average user). Since it was connected and running basically 24x7, I would have ample opportunities to gain access to the system without the users knowledge. I also thought that if this was a power user's machine maybe the user was administering financial servers or something critical to the company. To find out who was running the system, I started some keyboard logging to get login and passwords. Then I could log in on my computer with their information and gain access to their shared drives on a file server. This was safer than accessing their system to get around. Finding out that they were in fact a system's administrator for a critical system, I waited to see when that person might be away from their computer. When I was looking through their system, I found unique software used for administering certain critical systems. In turn, I couldn't use my computer for information gathering. So I started to do some staking out. For one week, I watched for patterns. I enabled keyboard logging and microphone recording. I found out that the user would get up and go to lunch consistently every day at 12:00 for one hour. The next week I checked some screen shots around lunchtime to see if they were still there and I called them. No response. I started the crack Session. I gave myself at least 30 minutes of available time assuming an hour lunch and providing for a safety factor. Within the 30-minute period, I used NetBus 2.1 to its fullest (see figures 4 – 10). I copied and remove files with file manager, had a financial application

© SANS Institute 2000 - 2005 Author retains full rights.

port redirected to mine, altered the registry so the person couldn't work anymore, etc., complete control.

After putting the computer back as it was and never once being discovered, I fully realized the threat that NetBus 2.1 poses, as an internal attack. The lesson learned was that I could push out the Trojan horse to other company department systems with ease. I knew that our company would probably scan emails coming into our network but not internal ones sent to other internal users. In addition, I knew that .dat files on desktops aren't consistently updated and laptops even less. Also, I knew that our laptops would be the easiest to compromise because the IT department is constantly fixing them. Thus, they have shared all directories to everyone so they could do the upkeep remotely. The scope of the threat was now apparent. All user desktops and laptops, internal servers, and gullible emailed individuals, such as consultants, using our network could be infected, ground to a halt and our company's production and livelihood could be at a stand still for a good length of time. In addition since our .dat files weren't up-to-date, I could place a newer Trojan horse on machines to create more backdoors and make the IT departments life miserable.

Okay, I think by now the tone of this paper shows that the author strongly believes that the program is still a valid Trojan horse threat. So what do you do if you think you have the server portion on your system? Here are some suggestions. Use the netstat command. It will show you all TCP (and UDP) sessions. Notice that you can see the session established with the high port, NetBus 2.1. Please note that some Trojan horse programs now come with randomly selected ports or ports that you can change. NetBus 2.1's standard port is 20034 but it is changeable. This makes it more difficult to identify if your system is infected because you can't key on a specific port being established as you could in the past. However, it is still a good idea to pick a time interval where you run a netstat command, for example every week. It's a fast free way to look into your system and what it's talking or connected to and if any abnormalities exist that warrants further investigation.

Netstat –an

TCP	169.133.24.182:1027	169.133.24.182:1043	ESTABLISHED
TCP	169.133.24.182:1032	0.0.0.0:0	LISTENING
TCP	169.133.24.182:1043	169.133.24.182:1027	ESTABLISHED
TCP	169.133.24.182:1579	0.0.0.0:0	LISTENING
TCP	169.133.24.182:1579	169.133.24.21:139	ESTABLISHED
TCP	169.133.24.182:1591	169.133.24.182:5057	TIME_WAIT
TCP	**169.133.24.182:20034**	**169.133.24.205:1397**	**ESTABLISHED**

Second, go into HKEY_Local_Machine\Software and do a find on NetBus. I have placed a screen capture (see figure 11 below) of where I found NetBus 2.1 in my registry (There are other registry key locations for NetBus). Then, delete all NetBus entries. An easier way of removing NetBus from the registry is to use either of the following products, Registry Detective and Registry Editor Plus (both are Internet freeware). Both are registry explorer products and are easy to search for all NetBus related entries.

© SANS Institute 2000 - 2005 Author retains full rights.

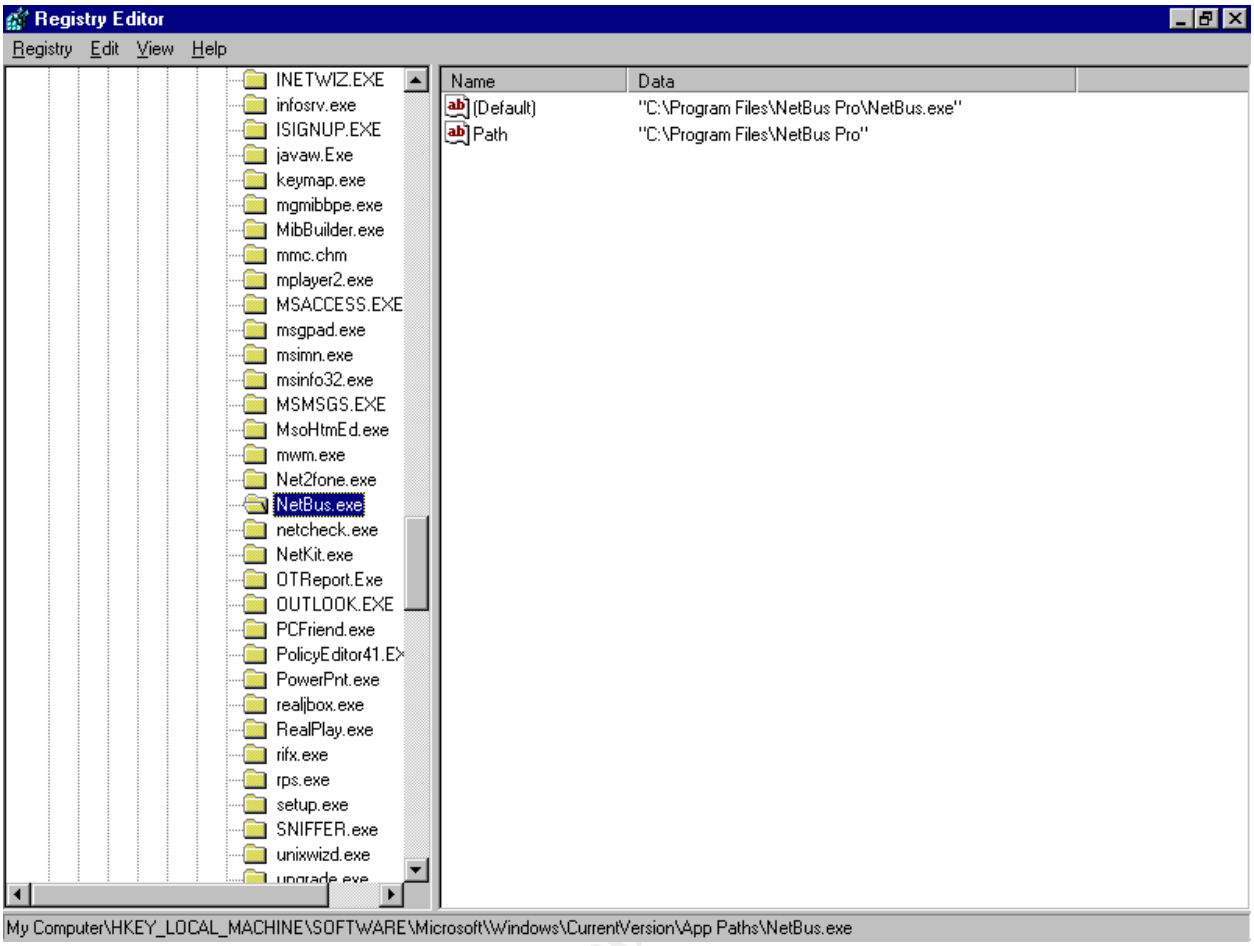


Figure 11: Screen Shot Windows 98 Registry NetBus 2.1

Another way of finding out if you are infected is to run the most current virus scans on your computers (not with NetBus 2.1). They will pick up most of the latest and greatest viruses and tell you how to remove them if you are infected. Finally (for this paper), try loading a host based Intrusion Detection System (IDS) for your desktops, laptops, servers, etc (please see Figure 12: ZDNet Security Downloads). Host based IDS's look for certain signatures and essentially prevent infections by keeping the host from receiving the signature code.

CONCLUSION

What can be concluded, from this author's point of view, is that NetBus version 2.1 is more of a legal threat than ever. Even though it cannot be stealthily installed anymore (as a Trojan horse would), it also won't show up on virus .dat files anymore. It does provide good remote administration. However, that remote administration can be undetectable by most users. Either by running the server invisible, keyboard logging, registry changes, etc., computer illiterate users don't stand a chance.

So one must have a good sound security policy that users follow. It will tell users what they can and cannot do. In addition, Users must be educated on what could be viewed as a threat not only from the exterior but also interior attacks. Many users feel that they are safe within the interior of a network and freely open internal and external email attachments without any hesitation, against our security policy. So not only educate your users on what they are allowed or not allowed to do within your network but keep them up to date on the latest attack attempts and what to look out for. With a constant

© SANS Institute 2000 - 2005 Author retains full rights.

security focus that branches out to all users, the security seed is planted, spread and always reinforced.

FOR FURTHER INFORMATION

If you think your system(s) have been compromised by any version of NetBus, don't panic. There is a ton of information on the Internet about all versions (some for 2.1). The following is a list where one can obtain further information on NetBus:

1. SANS Organization at www.sans.org.
2. FBI's NIPC (National Infrastructure Protection Center at www.nipc.gov.
3. Network Associate's McAfee at www.mcafee.com.
4. Symantec's Norton virus detection at www.norton.com.
5. To download NetBus versions try www.portwolf.com/trojans.htm. Note: there are a lot of places to acquire the software throughout the Internet.
6. ZDNet Downloads (see figure 12 below) at www.zdnetindia.com/downloads/utilities/stories/9218.html. See below for PC protection software.

Title	Date	Rating	OS
PC Detective Monitor your PC	23-OCT-00	★★★★★	Windows 9x, NT, or 2000
ZoneAlarm Protect DSL and cable modem systems	16-OCT-00	★★★★★	Windows 9x, NT, 2000, or Me
Jammer Lock your PC from outsiders	16-AUG-00	★★★★★	Windows 95 or Windows 98
Security Wizard 98 Keep your desktop computer secure	26-MAR-00	★★★★★	Windows 95 or Windows 98
Encrypted Magic Folders Hide and encrypt folders	16-SEP-99	★★★★★	Windows 95 or Windows 98
InoculateIT Personal Edition Protect your computer from viruses	23-OCT-00	★★★★	Windows 95, 98, or NT
PGP for Personal Privacy Encrypt files and email	08-JUL-97	★★★★★	Windows 95
Security Officer Professional Protect your PC on the Net and more	18-NOV-99	★★★★★	Windows 95, 98, or NT
Norton Personal Firewall 2000 Protect your PC from Internet intruders	22-JUN-00	★★★★★	Windows 9x, NT, or 2000
Security Tutorial Learn about security issues	26-MAR-97	★★★★★	Windows 3.1x

Figure 13: ZDNet Security Downloads

© SANS Institute 2000 - 2005 Author retains full rights.

REFERENCES

The American Heritage College Dictionary Third Edition. Dic.tion.ary, 1997 Houghton Mifflin Company. 1448.

The BASE Hack and Security Resources. "Backdoor.g", March 6 2001 URL: http://entraserver.hypermart.net/report/may20virus/backdoorg.html.

Joshua D. "The Trojan Horse", January 1996 URL: www.darter.ocps.k12.fl.us/classroom/who/darter1/trhorse.htm.

Kossakowski, Klaus-Peter. "Glossary of Computer Security Incident Handling Terms and Abbreviations." CERT. 6 March 2000. URL: http://www.cert.dfn.de/eng/pre99papers/certterm.html.

Members.nbci.com. "What is NetBus?", URL: http://members.nbci.com/_XMCM/sergiomili/what.html.

Netscams.com. "Win95.BackDoor.G", May 25, 1999 URL: www.netscams.com/alert/virusalerts/backdoor-g.html.

Nttoolbox.com. "The NetBus Threat", URL: www.nttoolbox.com/Netbus.htm.

Nwinternet.com. "NetBus BO's Older Cousin", October 13, 1998 URL: http://www.nwinternet.com/~pchelp/nb/netbus.htm.

SearchSecurity.com. "Trojan horse", May 10, 2001 URL: http://www.searchsecurity.techtarget.com/sDefinition/0,,sid14_gci213221,00.html.

© SANS Institute 2000 - 2005 Author retains full rights.

ZDNet India Downloads. " Secure your PC – Online and offline!," December 12, 2000 URL:
www.zdnetindia.com/downloads/utilities/stories/9218html.

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.