The Complete Windows Trojans Paper
By Dancho Danchev
dancho.danchev@frame4.com
http://www.frame4.com/

Version 1.0

Author's Notes:

This is the updated version of my paper written a long while ago. During that time I have seen it on every security/hacking site I came across and I'm glad you're all placing it in your archives as recommended reading. Now, many more sections and updates have been added so be sure that you will reading new and interesting aspects regarding the topic. The paper will answer many questions people keep asking in general about trojans like "how are attackers infecting me" and "how to protect from trojans".

If you have any other questions about the topic including ideas, suggestions, comments, etc., please do not hesitate to express your opinion. If you have a lot to say on the topic and/or I have missed some aspects then please contact me and contribute to the next update, and of course full credit will be given to you and your ideas.

Table of Contents

1.What is This Paper About?

The Complete Trojans Text is a paper about Windows Trojans, how they work, their variations and, of course, strategies to minimise the risk of infection.

Links to special detection software are included as well as many other topics never discussed before. This paper is not only intended to be for the average Internet/Windows user who wants to know how to protect his/her machine from Trojan Horses or just want to know about their usage, variations, prevention and future, but will also be interesting for the advanced user, to read another point of view.

Windows Trojans are just a small aspect of Windows Security but you will soon realise how dangerous and destructive they could be while reading the paper.

2.What Is A Trojan Horse?

A Trojan horse is:

- An unauthorised program contained within a legitimate program. This unauthorised program performs functions unknown (and probably unwanted) by the user.

- A legitimate program that has been altered by the placement of unauthorised code within it; this code performs functions unknown (and probably unwanted) by the user.

- Any program that appears to perform a desirable and necessary function but that (because of unauthorised code within it that is unknown to the user) performs functions unknown (and definitely unwanted) by the user.

The Trojan Horse got its name from the old mythical story about how the Greeks gave their enemy a huge wooden horse as a gift during the war. The enemy accepted this gift and they brought it into their kingdom, and during the night, Greek soldiers crept out of the horse and attacked the city, completely overcoming it.

3.How Do Trojans Work?

Trojans come in two parts, a Client part and a Server part. When the victim (unknowingly) runs the server on its machine, the attacker will then use the Client to connect to the Server and start using the trojan. TCP/IP protocol is the usual protocol type used for communications, but some functions of the trojans use the UDP protocol as well. When the Server is being run on the victim's computer, it will (usually) try to hide somewhere on the computer, start listening on some port(s) for incoming connections from the attacker, modify the registry and/or use some other autostarting method.

It's necessary for the attacker to know the victim's IP address to connect to his/her machine. Many trojans have features like mailing the victim's IP, as well as messaging the attacker via ICQ or IRC. This is used when the victim has dynamic IP which means every time you connect to the Internet you get a different IP (most of the dial-up users have this). ADSL users have static IPs so the infected IP is always known to the attacker and this makes it considerably easier to connect to your machine.

Most of the trojans use Auto-Starting methods so even when you shut down your computer they're able to restart and again give the attacker access to your machine. New auto-starting methods and other tricks are discovered all the time. The variety starts from "joining" the trojan into some executable file you use very often like explorer.exe, for example, and goes to the known methods like modifying the system files or the Windows Registry. System files are located in the Windows directory and here are short explanations of their abuse by the attackers:

- Autostart Folder
The Autostart folder is located in C:\Windows\Start Menu\Programs\startup and as its name suggests, automatically starts everything placed there. - Win.ini
Windows system file using load=Trojan.exe and run=Trojan.exe to execute the Trojan
- System.ini
Using Shell=Explorer.exe trojan.exe results in execution of every file after Explorer.exe
- Wininit.ini
Setup-Programs use it mostly; once run, it's being auto-deleted, which is very handy for trojans to restart
- Winstart.bat
Acting as a normal bat file trojan is added as @trojan.exe to hide its execution from the user
- Autoexec.bat
It's a DOS auto-starting file and it's used as auto-starting method like this -> c:\Trojan.exe
- Config.sys
Could also be used as an auto-starting method for trojans
- Explorer Startup
Is an auto-starting method for Windows95, 98, ME and if c:\explorer.exe exists, it will be started instead of the usual c:\Windows\Explorer.exe, which is the common path to the file.

Registry is often used in various auto-starting methods. Here are some known ways:

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]
"Info"="c:\directory\Trojan.exe"
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce]

"Info"="c:\directory\Trojan.exe"
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices]
"Info"="c:\directory\Trojan.exe"
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce]
"Info="c:\directory\Trojan.exe"
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]
"Info"="c:\directory\Trojan.exe"
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce]
"Info"="c:\directory\Trojan.exe"

- Registry Shell Open

[HKEY_CLASSES_ROOT\exefile\shell\open\command]
[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\exefile\shell\open\command]

A key with the value "%1 %*" should be placed there and if there is some executable file placed there, it will be executed each time you open a binary file. It's used like this: trojan.exe "%1 %*"; this would restart the trojan.

- ICQ Net Detect Method

[HKEY_CURRENT_USER\Software\Mirabilis\ICQ\Agent\Apps\]

This key includes all the files that will be executed if ICQ detects Internet connection. As you can understand,this feature of ICQ is very handy but it's frequently abused by attackers as well.

- ActiveX Component

[HKEY_LOCAL_MACHINE\Software\Microsoft\Active Setup\Installed Components\KeyName]
StubPath=C:\directory\Trojan.exe

These are the most common Auto-Starting methods using Windows system files, and the Windows registry.

4.Trojans Variations

There are so many variations out there, it will be hard to list and describe each and every one of them, but most are a combination of all the trojan features you will read about below, or have many other functions still not, and probably will never be known to the public.

Remote Access Trojans

These are probably the most publicly used trojans,just because they give the attackers the power to do more things on the victim's machine than the victim itself, while standing in front of the machine. Most of these trojans are often a combination of the other variations you'll read below. The idea of these trojans is to give the attacker a COMPLETE access to someone's machine, and therefore access to files, private conversations, accounting data, etc.

Password Sending Trojans

The purpose of these trojans is to rip all the cached passwords and also look for other passwords you're entering then send them to a specific mail address, without the user noticing anything. Passwords for ICQ, IRC, FTP, HTTP or any other application that require a user to enter a login+password are being sent back to the attacker's e-mail address, which in most cases is located at some free web based e-mail provider. Most of them do not restart when Windows is loaded, as the idea is to gather as much info about the victim's machine as passwords, mIRC logs, ICQ conversations and mail them; but it depends on the needs of the attacker and the specific situation.

Keyloggers

These trojans are very simple.The only one thing they do is to log the keystrokes of the victim and then let the attacker search for passwords or other sensitive data in the log file. Most of them come with two functions like online and offline recording. Of course they could be configured to send the log file to a specific e-mail address on a daily basis.

Destructive

The only function of these trojans is to destroy and delete files. This makes them very simple and easy to use. They can automatically delete all your core system files (for example: .dll, .ini or .exe files, possibly others) on your machine. The trojan is being activated by the attacker or sometimes works like a logic bomb and starts on a specific day and at specific hour.

Denial Of Service (DoS) Attack Trojans

These trojans are getting very popular these days, giving the attacker power to start DDoS if having enough victims of course. The main idea is that if you have 200 ADSL users infected and start attacking the victim simultaneously, this will generate a LOT of traffic (more then the victim's bandwidth, in most cases) and its the access to the Internet will be shut down. WinTrinoo is a DDoS tool that has become really popular recently, and if the attacker has infected many ADSL users, major Internet sites could be shut down as a result, as we've seen it happen in the past few months.

Another variation of a DoS trojan is the mail-bomb trojan, whose main aim is to infect as many machines as possible and simultaneously attack specific e-mail address/addresses with random subjects and contents which cannot be filtered.

Proxy/Wingate Trojans

Interesting feature implemented in many trojans is turning the victim's computer into a proxy/wingate server available to the whole world or to the attacker only. It's used for anonymous Telnet, ICQ, IRC, etc., and also to register domains with stolen credit cards and for many other illegal activities. This gives the attacker complete anonymity and the chance to do everything from YOUR computer and if he/she gets caught the trace leads back to you.

FTP Trojans

These trojans are probably the most simple ones and are kind of outdated as the only thing they do is to open port 21(the port for FTP transfers) and let EVERYONE connect to your machine or just the attacker. Newer versions are password protected so only the one that infected you may connect to your computer.

Software Detection Killers

There are such functionalities built into some trojans, but there are also separate programs that will kill ZoneAlarm, Norton Anti-Virus and many other (popular anti-virus/firewall) programs, that protect your machine. When they are disabled, the attacker will have full access to your machine, to perform some illegal activity, use your computer to attack others and often disappear. Even though you may notice that these programs are not working or functioning properly, it will take you some time to remove the trojan, install the new software, configure it and get back online with some sense of security.

I would like you to look at a list created by SnakeByte (nice work dude!):

http://www.snake-basket.de/e/AV.txt

Check it out and you will get my point how easily these programs could be disabled. It's a list of Anti-Virus detection software with its Window Names, associated files and many more things that attackers found as a way to disable certain protection software. I've seen only several anti-trojan packages that let the user specify another location of the program (installation) files, different from the default one, also Window names and many other features that will make it harder for the attacker to disable the software.

5.The Future Of Windows Trojans

Windows users will always be targets of malicious attackers because most of them don't know the real meaning of the word security, and think that some firewall is the only solution they need for protection but they actually don't have a clue how it works, or how to configure it properly. Windows Trojans will be a big security problem in the future and I'm sure attackers realise that, and many more unique functions will be implemented into their trojans but will mostly be used for the attacker's private purposes. Programmable or scriptable "automated hacking" functions will be used to solve various attacker's problems starting from anonymous port scanning and going up to Distributed Denial Of Service Attacks(DDoS). A recommended resource related to the subject is

http://staff.washington.edu/dittrich/misc/ddos/

How about distributed cracking of password files like on all of these contests around the world but in that case a network created by attacker/attackers for their own purposes? Has anyone ever thought of "spamming" function, built into trojans, similar to all of these spam programs out there, crawling around the Internet, searching for e-mails? And these are just small examples, but trust me, there are much more advanced features, built into Windows Trojans, that probably will never be released to the public.

At this year's Defcon the security company SensePost made a demonstration with a trojan, called Setiri, bypassing all the firewalls and IDS's giving access to the attacker even the machine was in a restricted environment. More info is available at:

http://www.computercops.biz/modules.php?name=News&file=article&sid=1321

6.How Can I Get Infected?

A lot of people out there can't differ various ways of infection just because in their minds the only way of getting infected is by downloading and running server.exe and they will never do it as they say. As you'll read here, there are many more ways for malicious attackers to infect your machine and start using it for illegal activities. Please take all of these topics I'm reviewing here really seriously; read them

carefully and remember that prevention is way better than the cure!

6.1 ICQ
6.2 IRC
6.3 Attachments
6.4 Physical Access
6.5 Browser And E-mail Software Bugs
6.6 Netbios(FileSharing)

6.1 Via ICQ

People don't understand that they can also get infected while talking via ICQ or any other Instant Messenger Application. It's all risky when it's about receiving files no matter from who, and no matter from where.

Believe it or not, there are still guys out there, using really old versions of ICQ and it's all because they can see the IP of the person they're talking to. The older versions of ICQ had such functionality and it was useful for everyone capable of using winnuke and other DoS tools, but really how hard it is to click with the mouse? These people are often potential victims of someone that is more knowledgeable on Windows Trojans and takes advantage of their old ICQ versions.

Let's review various ways of getting infected via ICQ:

- You can never be 100% sure who's on the other side of the computer at the particular moment. It could be someone that hacked your friend's ICQ UIN (Unique Identification Number)and wants to spread some trojans over his/her friends. You'll definitely trust your best dude Bob if he offers you something interesting, but is it really Bob on the other side?

- Old versions of ICQ had bugs in the WebServer feature, that creates a site on your computer, with your info from the ICQ database. The bug consists in that the attacker can have access to EVERY file on your machine and if you read the previous sections carefully and know the auto-start methods, you'll probably realise what could happen if someone has access to your win.ini or other system file, namely a trojan installed in a few minutes.

- Trojan.exe is renamed like Trojan....(150 spaces).txt.exe, icon changed to a real .txt file and this will definitely get you infected. This bug must be fixed in the newer versions for sure.

No matter which Instant Messenger Application you're using, you could always get yourself infected by certain program bug you never had the chance to hear about, and never took care of checking for newer versions of the application, also when it's about receiving files no matter where, and no matter from who, take that very seriously and realise the dangers of your naivety.

6.2 Via IRC

So many people LIVE on IRC and this is another place where you can get yourself infected. Trust is vital no matter what you're doing. No matter who is sending you files, pretending to be free porn archive, software for "free internet", hacking Hotmail program, DO NOT get any of these files. Newbies are often targets of these fakes, and believe me, many people are still newbies about their security. Users get infected from porn-trade channels, and, of course, warez channels, as they don't think about the risk, but how to get free porn and free programs instead.

Here are several scenarios of you getting infected while using IRC:

- You're talking with someone, a "girl" probably, have great time and, of course, you want to see the person you're talking to. You ask for a picture or the "girl" offers you her pictures and I'm sure you'll definitely want to see them. The "girl" says that she has just created her first screensaver, using some known free or commercial software to do this, and offers it to you, but how about if "she" mentions several pictures are naked ones?! You have been talking to "her" for a week or so, you get this screensaver.exe, you run it and, yeah, VERY nice pics, some are naked and she didn't lie to you so nothing bad or suspicious has happened BUT think again what really has happened!

- Trojan.exe could also be renamed into Trojan.scr like a screensaver extension and will again run properly when you execute it so pay attention about these file extensions.

- Trojan.exe is being renamed like Trojan....(150 spaces).txt.exe you'll get the file over IRC in the DCC it will appear as .TXT and you won't get worried about anything, run it and get yourself infected again. In all of these examples the icon of the file is changed, of course, because it needs to be the same icon as a normal .TXT and this fools victims very often.

Most people don't notice in their Explorer that the Type of the file is Application BUT with a .TXT icon. So BEFORE you run something, even if it's with a .TXT icon, check its extension and make sure it's really a text file.

6.3 Via Attachments

I'm always amazed how many people got themselves infected by an attachment, sent into their mailboxes. Most of these users are new to the Internet and are pretty naive. When they receive a mail,containing an attachment, saying they will get free porn, free Internet access etc., they run it without completely understanding the risks for their machines. Check the following scenario: you know your friend Alex is a very skilled Visual Basic programmer. You also know he's coding his latest program but you're curious what it is all about, and you wait for an e-mail from him with the attachment when he finishes coding the application. Yeah, but the person targeting YOU also knows that. The attacker also knows your friend's e-mail address. Then the attacker will simply code some program or get some freeware one, use some relaying mail server to fake the e-mail's FROM field and make it look like your friend's one; Alex's e-mail address is alex@example.com so the attacker's FROM field will be changed to alex@example.com and, of course, it will include the TROJANED attachment... You'll check your mail, see that Alex finally got his program ready and sent it, you'll download and run it without thinking that it might be a trojan or something else, because, hey, Alex wouldn't do something like that to me, he's my friend, and you'll get yourself infected.

Information Is Power! Just because the attacker knew you were waiting for some particular file, he found Alex's e-mail address and got you infected... the right moment assumes importance here. And it all happened just because you were naive, just because you saw alex@example.com in the FROM field, and just because you didn't check the mail headers to see that the mail came from some .jp mail server relaying e-mails and, has been used from spammers for several months.

Many people got themselves infected by the famous "Microsoft Internet Explorer Update" sent directly to their mailboxes, by the nonexistent Microsoft Updates Staff. I understand you felt great because Microsoft are paying attention especially to you, and sent you the latest updates, but these "updates" are definitely trojans. Microsoft will NEVER send you updates of their software via e-mail no matter you see the FROM field is updates@microsoft.com and as you've noticed in the previous example the

FROM field could and IS faked. If you ever notice some mail in your mailbox with subjects like "Microsoft IE Update" and such, delete WITHOUT viewing or reading the e-mail, because some E-Mail clients like Outlook Express and others, have bugs that automatically execute the file being attached in the e-mail WITHOUT you even touching it. As you can imagine this is a extremely dangerous problem that requires you to be always up to date with the latest version of any software you're using.

6.4 Physical Access

Physical access is vital for your computer's security. Imagine what can an attacker do while having physical access on your machine, and let's not mention if you're always connected to the Internet and leave the room for several minutes... long enough to get you infected. Here I'll point you several scenarios, often used by attackers to infect your computer while they're having physical access to your machine. There are some very smart people out there that keep thinking of new ways of getting physical access to someone's computer. Here are some tricks that are interesting:

- Your "friend" wants to infect you with a trojan and he/she has physical access to your machine. Let's say you were at home surfing the net, chatting or whatever. Suddenly your "friend" asks you for a glass of water, knowing that you'll go in another room and will be away for 1 or 2 minutes. While you do that he/she takes out a diskette of the pocket and infects your unprotected PC. You came back and everything is OK because your "friend" is doing exactly the same thing before you left ...surfing the net.

- The next example is when 2 guys want to take revenge on you cause of something and are supporting each other to accomplish the task. Again you are at home with your "friend", surfing, chatting, whatever you're doing; suddenly the telephone rings and a "friend" of yours wants to speak with you for something that is really important. He/she (it's better to be she in this case) asks "Is there anyone around you? If so,please move somewhere away from him/her(after knowing it is him or her,of course). I don't want anyone to listen what I'm going to tell you". The victim is again lured away from the computer, leaving the attacker to do whatever he/she wants on the target computer.

- Other approaches like the previous ones might be sudden ring on the bell, as well as other variations of phone calls and conversations leaving the attacker alone with the victim's computer. There are so many other possible approaches; just think for a while and you'll see what I mean and how easily you could be tricked, and it's because you're not suspicious enough when it is about your sensitive computer data.

- Another way of infecting while having physical access is the Auto-Starting CD function. You've probably noticed that when you place a CD in your CDROM, it automatically starts with some setup interface; here's an example of the Autorun.inf file that is placed on such CD's:

```
[autorun]
open=setup.exe
icon=setup.exe
```

So you can imagine that while running the real setup program a trojan could be run VERY easily, and as most of you probably don't know about this CD function they will get infected and won't understand what happened and how it's been done. Yeah, I know it's convenient to have the setup.exe autostart but security is what really matters here, that's why you should turn off the Auto-Start functionality by doing the following:

Start Button -> Settings -> Control Panel ->
System -> Device Manager -> CDROM -> Properties -> Settings

and there you'll see a reference to Auto Insert Notification. Turn it off and you won't have any problems with that function anymore.

I know MANY other variations of physical access infections but these are the most common ones so pay attention and try to make up several more by yourself.

When the victim IS connected to the Internet:

Here we have many variations; again, I'll mention the most common ones. While the attacker is having physical access he/she may download the trojan.exe, using various ways just by knowing how various Internet protocols work.

- A special IRCbot known only to the attacker is staying in IRC with the only function to DCC the trojan.exe back to the attacker whenever he/she messages the bot with a special command. The victim will probably be away from the computer.
- The attacker wants to download some specific software like new version of some programs infected with trojan(s), of course, and visit some URL, known to him/her only, and download the trojan.
- The attacker pretends he/she wants to check his/her (web based) mail (for example, at Yahoo! or HotMail) but in fact has the trojan.exe stored in his/ her mailbox and just downloads and executes the file, hereby infecting the computer. The mail service is used as a storage area, in this case.

There are many more ways of infecting the victim while connected to the Net, as you can imagine. Any of these examples will succeed but it all depends on the victim's knowledge of the Internet and how advanced his/her skills are, so the attacker needs to check these things somehow before doing any of these activities I pointed here. After that, the attacker will be able to choose the best variant for infecting the victim and doing the job.

6.5 Browser And E-mail Software Bugs

Users do not update their software versions as often as they should be, and a lot of the attackers are taking advantage of this well known fact. Imagine you are using an old version of Internet Explorer and you visit a (malicious) site that will check and automatically infect your machine without you downloading or executing any programs. The same scenario goes when you check your E-mail with Outlook Express or some other software with well known problems, again you will be infected without downloading the attachment. Make sure you always have the latest version of your Browser and E-mail Software, and reduce the ways of these variations to minimum. Here are some links about Browser and E-mail Software bugs, check them out and understand how dangerous these bugs are, and it's all because of you using an old version of the software.

http://www.guninski.com/browsers.html
http://www.guninski.com/netscape.html

6.6 Netbios(File Sharing)

If port 139 on your machine is opened,you're probably sharing files and this is another way for someone to access your machine, install trojan.exe and modify some system file, so it will run the next time you restart your PC. Sometimes the attacker may use DoS(Denial Of Service Attack) to shut down your machine and force you to reboot, so the trojan can restart itself immediately. To block file sharing in WinME version, go to:

Start->Settings->Control Panel->Network->File And Print Sharing

and uncheck the boxes there. That way you won't have any problems related to Netbios abuse.

7.Fake Programs

Imagine a Freeware SimpleMail program that's very suitable for your needs, and very handy with its features like address book, option to check several POP3 accounts and many other functions that make it even better then your E-mail client and the best thing for you is that it's free. You use ZoneAlarm or any other similar protection software, and mark the program as a TRUSTED Internet server so none of your programs will ever bother you about that program as you are using it probably every day because it's working very well, no problems ever occurred, you're happy, but a lot of things are going in the background. Every mail you send and all your passwords for the POP3 accounts are being mailed directly into the attacker's mailbox without you noticing anything. Cached passwords and your keystrokes could be also mailed and the idea here is to gather as much info as possible and send it to the attacker. This info includes credit card numbers, passwords for various applications and many other things.

In some cases the attacker may have complete access to your machine but it depends on his/her ideas about the hidden program's functions. When sending e-mails and using port 25 or 110 for POP3, these could be used for connections from the attacker's machine (not at home, of course, but again from another hacked one) to connect and use the hidden functions he/she implemented in the Freeware SimpleMail. The attacker's idea here is to offer you a program that requires a connection to be established with some server; let's say at the top of the SimpleMail there's a banner that's auto-refreshing every few minutes, because the programmer "needs to pay the bills too" as he said in the About section, so nothing seems suspicious to you as it's a normal thing, and your logical conclusion is completely right as the only way for that guy to keep offering this cool freeware program for free is to use banners. You've already marked the program as TRUSTED so the attacker can have complete access to your machine because he/she fooled you into thinking it's a TRUSTED program. Even if you notice some connection to your machine on some strange port, you won't consider this as a suspicions event, as the banners section needs to get these banners from somewhere, and this is the place your machine is connected all the time to keep them refreshing.

The only thing the attacker needs is creativity, and most of them do have it. Think of a fake AudioGalaxy (software for mp3's sharing) but, of course, with a different name. The attacker would create it, will free 15GB disk space on his machine and place a large archive of mp3's...then, of course, the same will be done on several other machines to fool you that you are downloading from other people located all over the world, but it's not necessary as the program's interface may never show you where you're actually downloading the mp3's from. The software will again be backdoored as in the previous example, and will get thousands of naive users, probably using ADSL connections, infected.

Fake programs that have hidden functions, often have professional looking web sites, links to various anti-trojan software mentioned as affiliates, and make you trust the site; readme.txt is included in the setup and many other things to fool you it's a trusted one. Pay attention to freeware tools you download, consider them extremely dangerous and a very useful and easy way for attackers to infect your machine with a Trojan.

8.Untrusted Sites And Freeware Software

A site located at some free web space provider or just offering some programs for illegal activities can

be considered as untrusted one. As you know, there are thousands of "hacking/security" archives on these free web space providers like Xoom, Tripod, Geocities and many many others. These sites have archives full with "hacking" programs, scanners, mail-bombers, flooders and many other tools. Often several, if not all of these programs are infected by the guy who created the site. It's highly risky to download any of the programs and the tools located on such untrusted sites; no matter which software you use are, you ready to take the risk? There are some untrusted sites, looking REALLY professional and having huge archives, full with Internet related software, feedback form, links to other popular sites. I think if you take some time, look deeper, scan all the files you download you can decide on your own whether the site you are downloading your software from is a trusted or an untrusted one.

Software like mIRC, ICQ, PGP or any other popular software MUST be downloaded from its original (or official dedicated mirror site) and not from any of these I told you about. Sometimes such sites claim there's a new version of, let's say, mIRC 7.0, and you know your current version is 6.0 and, yeah, it's handy to click on the URL and download the .exe in 1 minute and take advantage of the latest version, but will definitely get yourself infected. A possible variation of this method will again be claiming for a new version, BUT the site would include info on nonexistent security bugs, found in the previous one (which is of course the latest you have), and again it is handy for you to download it, instead of visiting mIRC's main site, and see if there is really an updated version or check for any of these security bugs you've read about on the fake site.

Webmasters of well known Security Portals, that have HUGE archive with various "hacking" programs, should be responsible for the files they provide and OFTEN scan them with Anti-Virus and Anti-Trojan software to guarantee their visitors download "free of trojans and viruses". A known method is that attackers send some program created by them, let's say a UDP flooder, to the webmaster like a submission for the archive, but infect the program with some trojan and later have visitors downloading the program and getting themselves infected. Some attackers may use the webmaster's irresponsibility and infect their files, and have the site distribute the trojan. I know of another story regarding this problem. It's about a Gaming Magazine that used to include a CD with free demo versions of the latest games in each new edition. The editors made a contest to find new talents and give the people programming games the chance to popularise their productions by sending them to the Editors. An attacker infected his game with a new and private trojan and sent it to the Magazine. In the next edition the "game" appeared on the CD and you can imagine the chaos that set in. And it's all because of the Editors, having not so much knowledge on the topic and as I've told you, in the old days Anti-Virus software were detecting only a small part of the public trojans (and what about all the private ones). In this particular case they were using only an Anti Virus scanner to protect their readers from such attacks. Webmasters and everyone having some sort of software archive on his/her portal, MUST scan it very often, and before adding a new file it should be well examined; if it's suspicious in any way, it must be sent to your software detection labs for further analysis. Do care about your visitors/readers if you want them to care about you.

Freeware programs could be considered suspicious and extremely dangerous, due to the fact that it's a very easy and useful way for the attacker to infect your machine with some freeware program. No matter how suitable you find the program, remember that "free is not always the best" and it's very risky to use any of these programs. My advice is: before using Freeware program, do search for some reviews on it, check popular search engines, and try to look up for some info about it. If you find any reviews written by respected sites, that means they've used and tested it and the chance of infection is hereby, minimised. If no reviews or comments about the software are found via the search engines, then it may be highly risky to start using it.

9.How Are They Detecting My Internet Presence?

People new to the Internet often ask this question as they can't understand why someone will want to attack especially them, because they never did any harm to anyone and never did something that might get them into trouble. While reading the previous sections, I hope you understood that sometimes you only need to visit a web site with your unpatched browser and get yourself infected.

I will explain several scenarios on how attackers may discover your Internet presence:

- When visiting a web page,the attacker might have created a script that will automatically check your Browser for known bugs, and if any are detected, install a trojan on your machine or notify the attacker to have a deeper look. Make sure you're always using the latest version of your Browser for maximal protection. Check for (security) patches and apply these often! - When joining an IRC channel, an IRC bot might be configured to scan everyone joining for specific trojan ports opened or FileSharing (Netbios) enabled. If the attacker is smart, the script will scan you several minutes after you join the channel and, of course, use an IP number not belonging to anyone in the channel.
- Attackers often attempt IP blocks scanning, looking default trojan ports and of course FileSharing (Netbios). After infection, your machine could also be used for such scans, as well as an IRC bot, scanning those joining some big and full with people IRC channel.

These are some of the most common ways attackers use to search for new victims, suitable for their illegal activities. If someone is targeting especially you, the attacker won't be using any of these methods I reviewed above; instead your Browser version will be found as well as the Operation System you're using, and the attacker will make a personal contact with you via IRC, ICQ, etc., and fool you somehow and get you infected.

10.What Is The Attacker Looking For?

Some of you may think that trojans are used for damages only. Well, they can also be used for spying on someone's machine and taking a lot of private and sensitive information (industrial espionage). The attacker's interests would include but are not limited to the following:

- Credit Card Information (often used for domain registration, shopping with your credit card)
- Any accounting data (E-mail passwords, Dial-Up passwords, WebServices passwords, etc.)
- Email Addresses (Might be used for spamming, as explained above) - Work Projects (Steal your presentations and work related papers) - Children's names/pictures, Ages (pedophile attacker?!) - School work (steal your papers and publish them with his/her name on it)

I'll mention again several scenarios about the attacker's mode of thinking:

- Once infected, your computer might be used as a Warez Archive. No matter how much or little free disk space you have, you'll probably have enough for the attacker's needs. He/she won't use all of your bandwidth; there will be some limit for connections to your computer, so you'll still be able to do your work without knowing that your computer is used as a pirated software FTP Server and it is known to people worldwide who keep downloading software from YOU.
- Kiddie-Porn traders will also use your computer for storing their archives and again turning your machine into a well known place for traders of nasty and above all illegal pictures. You'll again do your work and have no clue there are illegal activities going in your computer. - The attacker might just want to have fun with you, open/close the CD tray, play with your mouse, annoy you somehow; that's stupid and useless but a lot of people do it.
- Your computer might be used for other illegal purposes like the attacker's usage of your IP address to hack, scan, flood, infiltrate other machines on the Internet; so the victims will see your machine is doing

it, and this will definitely get you in trouble.

11.Intelligence With Trojans

Think for a while about how much your life depends on your computer, your ICQ, your chat program, your e-mail address and think how vulnerable your life is just because you're infected with a Trojan Horse. They can, and they have been used for intelligence for a very long time. Just by reading your e-mails, keeping track of your contacts, reading your private conversations, the web sites you visit, ICQ history, mIRC log files with your private conversations and a log of everything you do online, a psychological profile could be created in several hours (depends of the skills of course) and your life, mode of thinking, reactions on specific future situations and needs will be revealed to some geek, wanting to recruit and/or manipulate you. This is food for thought and another topic, but just think how a combination of psychology, social engineering and computer security knowledge makes you a really powerful guy. And remember that people reveal their REAL personalities, wishes, mode of thinking, interests only when they think nobody is watching them...

12.Trojan Ports

Trojans use specific ports to communicate with the client. In the old days the well known trojan ports were mostly used, but today it's possible to change the port every time the trojan is restarted. Here is a link to the best and probably including all of the public trojans Ports List I've come across.

http://www.simovits.com/trojans/trojans.html

13.How Do I Know I'm Infected?

Sometimes you think it's normal Windows behaviour when there are 500 MB or so missing on your HDD, because some software is using it, or you have installed a game you forgot about and many other reasons but not the real one. Here are some things which are very suspicious, and no matter how much your Anti-Virus software tells you that you aren't infected, dig a little deeper and see what really happened. One thing that will help you is to know the main features of the public trojans, so you'll be able to react if you notice such activity on your PC. I have included links to various Trojan Databases that you should visit if you want to know the main features of the public ones.

- Its normal to visit a web site and several more pop-ups to appear with the one you've visited. But when you do completely nothing and suddenly your browser directs you to some page unknown to you, take that serious.

- A strange and unknown Windows Message Box appears on your screen, asking you some personal questions.

- Your Windows settings change by themselves like a new screensaver text, date/time, sound volume changes by itself, your mouse moves by itself, CD-ROM drawer opens and closes.

Please note that most advanced attackers will just spy on you and use your infected machine for some specific reason, and not perform any of the above "tricks" so as not to cause any suspicious activity on the target system (as this would probably mean they could get easily detected). Someone that just wants to have fun with you is more likely to perform these actions.

14.Anti-Virus (AV) Scanners

In the old days Virus Scanners used to detect only viruses and just a small part of the public trojans on the Internet. Realising how dangerous and popular Trojans are becoming today most, if not all of these scanners detect probably all of the public ones out there. As always people, think they are safe and secure when using Virus Scanner but it's a false sense of security. This type of software relies mainly on "signatures" of each trojan's server executable and also its common auto-starting methods, but that is not the perfect solution by far for protection yourself against trojans, as they use many other methods to hide inside the machine, most of which are undetected by Anti-Virus Software. When trojans became a big security breach, specific Anti-Trojan packages were released to the public and it was necessary for the AVs to start detecting not only viruses, but also trojans if they wanted new users. As a result, most of them became really advanced trojan scanning and detection systems, but for your maximal protection it's recommended to use both Anti-Virus and Anti-Trojans software.

Public trojans appear online almost every day and the detection software is updated every day for maximal protection of its customers. One very big problem is that the users do not update their signature files as often as they should be, thus having detection software that's not detecting several more trojans or viruses. Users MUST update their software's signature files every day, and it will take them only several minutes. Each and every time a new file is downloaded, it MUST be scanned BEFORE being opened with Anti-Virus and Anti-Trojan software. If you think the file is suspicious due to some reasons, do NOT run it, but send it to your detection software labs for analysis.

15.Anti-Trojan Software

Here are reviews of the most popular Anti-Trojan packages. The list also includes various applications (freeware) to help you monitor your computer for ongoing Trojan activities. I suggest you visit the site of every product and decide which one best fits to your needs. Check the links section at the end of the paper to see various sites, providing reviews of the software below.

-- TDS-3 --

Trojan Defence Suite (TDS) is a indispensable, must-have software package for protection against trojans. It has many unique functions never seen in other Anti-Trojan packages. The program has really advanced features and if you're a newbie, it will probably take some time before you are able to use the software at its full capacity (read the excellent help files).

You can get TDS from http://tds.diamondcs.com.au/

-- LockDown2000 --

This is really good Anti-Trojan package that detects a LOT of trojans and other known as "hacking tools" programs. It will help you monitor your system files for changes, processes and registry modification. More info at its home page.

You can get LockDown2000 from http://www.lockdown2000.com

-- TFAK5 --

Trojans First Aid Kit is a trojan-scanner developed by SnakeByte. It has many other unique features; it could be used as a Client for various public trojans as well.

Download TFAK5 from http://www.snake-basket.de/tfak/TFAK5.zip

-- Trojan Remover --

Anti-Trojan software detecting 5468 trojans/worms (including variants) as at 15th August 2002. Systems files and registry monitoring functions are also implemented. More info at its home page:

http://www.simplysup.com/tremover/details.html

-- Pest Patrol --

A tool that scans for trojans as well as programs known as "hacking tools" and spyware. More info at its official page:

http://www.safersite.com/

-- Anti-Trojan 5.5 --

Trojans detection package that is able to remove most of the public trojans out there. More info at its official page:

http://www.anti-trojan.net

-- Tauscan --

Trojan scanner that has unique features and is a must have. It's also able to detect new and never released to the public trojans. More info at its official page:

http://www.agnitum.com/products/tauscan/

-- The Cleaner --

Very popular Anti-Trojan software, known by everyone. Check its home page at:

http://www.moosoft.com/

-- PC Door Guard --

Trojan detection software, detecting a lot of trojans, and a monitor of files and directories is also included. More info at:

http://www.trojanclinic.com/pdg.html

-- Trojan Hunter --

Trojan detection package with a lot of functions. It's very handy.

More info at http://www.mischel.dhs.org/trojanhunter.jsp

-- LogMonitor --

Log Monitor is a file and directory monitoring tool. The program periodically checks a selected file's modification time and executes an external program if file's time was changed or not changed. For directories it handles such events as files change, addition or removal. I recommend this tool as it's vary handy and will help you a lot.

Home page: http://logmon.bitrix.ru/logmon/eng/

-- PrcView --

PrcView is a freeware process viewer utility that shows detailed information about running processes. This information includes such details as the create date/time, the version and full path for each DLL used by a selected process, a list of all threads, memory blocks and heaps. PrcView also allows you to kill and attach a debugger to a selected process. PrcView runs on both Windows 95/98 and Windows NT platforms and includes Windows and command-line versions of the program.

Get PrcView from http://www.xmlsp.com/pview/prcview.htm

-- XNetStat --

GUI based netstat tool for Windows. It will help you monitor you machine for open ports. Download it from:

http://packetstormsecurity.org/Win/netstat.zip

-- ConSeal PC FIREWALL --

A really good firewall for advanced users using Windows having basic knowledge of TCP/IP and other protocols; this software will help you to secure your PC a lot. It has some major advantages over other Win based firewalls. For the full range of specifications, check its official web page at:

http://www.consealfirewall.com/

16.After You Clean Yourself

Your machine has been compromised and probably a lot of sensitive data stolen, files have been modified and illegal activities have been preformed on your computer. Here I'll give you recommendations about what to do after you are 100% clean of trojans.

- Accounting Data such as ISP passwords, ICQ, mIRC, FTP, web site passwords, e-mail address passwords are definitely known to the attacker. Contact your ISP about changing your dial-up password if you're using such connection. Immediately change your ICQ, mIRC passwords of course if they're still the same. (Often attackers won't change any of your accounting data to fool you everything is OK so there is a big chance you will still be able to recover from the compromise). Change your web based e-mail passwords and do check your information stored there, as password retrieval services for various e-mail providers such as Yahoo and Hotmail use this info combined with a "Secret Question" for password retrieval. Attackers often change the info, the answer to the secret question and many other things that will get them easily back into your mailbox, whether you've changed your pass or not.

- If you're taking advantage of the handy Address Book feature in your e-mail service, and have a list full of e-mails of friends, colleagues, etc. there is a real possibility that the attacker has sent them a

trojan and possibly infected them too. Mail all of these people and ask them about receiving any files from your mailbox, inform them someone else might know your e-mail password so they'll be able to take appropriate actions like checking their machines for Trojans. Do the same with the people from your ICQ contact list as they might be targeted too.

- Check your HDD for abnormal activities like a lot of free space missing etc. Search for warez software and, as I mentioned, kiddie-porn archives.

- Think for a while about the sensitive information you had on your machine before the compromise, and if you are absolutely sure the attacker may know it too, then take appropriate action, like informing the any institutions the sensitive data belong to.

- Scan your machine with Anti-Virus scanner, as the attacker could have placed some virus or infected macro documents on your machine to do destructive things even there's no access for him/her to your machine.

- Monitor your processes BEFORE and AFTER connecting to the Internet, as some trojans start when they detect Internet connection. Don't get fooled again, be very suspicious.

17.Online Scanning Services

These services are very popular these days and they are very handy for users who haven't got much knowledge on all of the holes they're checking for, but wanting to ensure they are protected from all of them. This section is placed at the end of the paper with a specific reason. If you have read the paper, you should know a LOT about trojans by now, their principles of working and detection techniques, therefore you can decide whether these online scanners are useful or if they give a false sense of safety.

There are several types of Online Scanners: Trojan Scanner, Port Scanner and Bugs Checker.

- Trojan Scanner
It's using a list with predefined ports, associated with the name of the trojan responding to its default port, like Girl Friend=21544, and if this port is in "listening" state on your machine it will inform you that you've been infected with the GirlFriend Trojan. As you already know, trojans have functions like changing their default port to ANY of the attacker's choice. That makes these Trojan Scanners kind of useless, because serious attackers do change the default port for sure.

- Port Scanner
This service has two options like well-known ports scan and all ports scan. The first feature is scanning for well known ports, again associated with the appropriate service related to the port like port 21-FTP, 23-Telnet, 25-SMTP. The second feature is rarely seen on a free one, because of the bandwidth it would generate to scan all of the 65,535 ports. It will again associate ports with services like I mentioned above, and if it finds any unknown ports not associated with any service, it will also report it, like Port 34525 State:Listening, which means this port is waiting for connections from the outside.

- Bugs Checker
Its purpose is to check your Browser or your E-mail Software for well known bugs and security related problems. If any are detected, it will point you to a site containing the patches for these bugs or a site with the latest updated versions of the software.

It's strongly recommended to close any other Internet related application on your machine before being

scanned by Online Trojan Scanner and Port Scanner. You decide which service is best for you, which one will be able to detect trojan infections on your machine, and which won't; you now know the main principles and the answers too, I hope. Links to several online scanning services I know of are included in the Links Section.

18.Advice

This is a very useful section, full of tips and advice on how to protect yourself from trojans using various ways you've already read about, but summarised here for faster reading and hopefully better understanding.

[01] Never accept a file even it is from some friend. You're never sure who's on the other side of the computer at the moment. If you really need this file, let's say some presentation or a work paper, find other ways, like the phone, and verify the file is from your friend. Yeah it will take you some time and slow you a bit, but be paranoid about attachments you may receive and don't get infected.

[02] When executing files, first check their type. Is it really a .doc or it's some executable with a .doc icon.

[03] Update your Anti-Virus and Anti-Trojan package signature files regularly, if possible EVERY day for maximal protection, as new trojans and viruses are discovered every day. Most of the detection software have functions
like scheduling scans so if you are away from your machine during the night but you leave it switched on, why not consider to schedule a scan and update every night? Doing so will ensure your maximal protection.

[04] Make sure you always have the latest version of the software you're using as new bugs appear very often and programs are regularly updated. Check often to see if there are bugs and/or other problems found in software
that may potentially expose your system to risk - and patch/update your system(s) accordingly. Some software have an option to check for the latest version of the software from the vendor web site; make use of it.

[05] Take several minutes and regularly check the processes on your machine with the software I reviewed above. You'll be surprised what you may
detect sometimes.

[06] It's vital to understand the risk of getting software from someone you just met, or had only several ICQ, IRC conversations with.

[07] Consider freeware programs as very risky software to download, and try searching for some reviews of the program before running it.

[08] Carefully read the help files coming with your detection software to be able to use them to their full capacity.

[09] Download software ONLY from its official page(s) or dedicated mirror web site. Never get the latest version of mIRC or ICQ from some site you've
never heard about like from some free web space provider like Geocities.
Consider it as an untrusted site and do NOT download anything from there.

[10] If you are playing with trojans you can also get infected as there are trojans or other software that are already infected and is waiting for
someone with not so much knowledge on the topic to download and use it.

[11] Don't be so naive on everything you see on the Internet or what various sites offer you - don't download some software you've never heard about.

19.Links Section

This section will be very useful for everyone interested in reading various papers about trojans written by other people, anti-trojan software reviews sites, trojans archives, trojan protection portals and many other sites related to the topic. If you want me to add your link in the next update mail me and if the site is somehow related to the topic, I will definately include it in the list.

Please don't forget that you can find these and many other security related links at our extensive web links directory at Frame4 Security Systems; check it out at: http://www.frame4.com/php/modules.php?name=Web_Links

-- Trojan Portals and Archives --

URL : http://www.tlsecurity.net
DESC : Excellent, well-known security portal providing many trojan resources and information regarding the topic

URL : http://www.euyulio.org
DESC : Security portal, huge trojans archive and other unique features

URL : http://www.megasecurity.org/
DESC : Megasecurity portal having huge trojans archive and well sorted library on the subject

URL : http://www.trojan.ch
DESC : Trojans portal, news, archive, unique programs

URL : http://www.trojanforge.net/
DESC : Trojans portal, trojans archive, documents, www-board

URL : http://packetstormsecurity.org/trojans
DESC : Packetstorm's trojans section

URL : http://www.pcflank.com
DESC : Security portal providing various functions as browser tests, remote trojan scanning

URL : http://www.staff.uiuc.edu/~ehowes/trojans/tr-tests.htm
DESC : Site showing results of actual (functional comparison) tests performed with various trojan detection programs

-- Trojan Database Libraries --

URL : http://www.simovits.com/trojans/trojans.html
DESC : Huge, detailed and well sorted list of trojans and their functions

URL : http://www.tlsecurity.net/tlfaq.htm
DESC : Comprehensive list and analysis of probably all the public trojans

URL : http://www.blackcode.com/trojans/
DESC : Trojans/worms library database provided by BlackCode

-- Anti Trojan Sites --

URL : http://www.hackfix.org/
DESC : Site with resources related to trojan protection and helping newbies

URL : http://www.nohack.net/
DESC : The nohack project helps newbies clean their PCs and protect themselves

URL : http://www.virushelp.info
DESC : IRC channel related to virus and trojans protection

URL : http://www.anti-trojan.org
DESC : Anti-trojan help site

-- Detection Software Reviews --

URL : http://www.wilders.org/anti_trojans.htm
DESC : Site providing reviews of anti-trojan software

URL : http://www.rokopsecurity.de/
DESC : German site providing reviews of various anti-virus and anti-trojan software, and many other information (site language is German)

URL : http://www.fruitloop.net/virushelp/index.html
DESC : Site providing reviews of detection software

URL : http://www.firewallguide.com/anti-trojan.htm
DESC : Site providing various security related services and reviews

-- Papers Regarding Windows Trojans --

URL : http://www.jmu.edu/computing/info-security/engineering/issues/remote.shtml
DESC : Interesting paper about windows trojans

URL : http://members.ozemail.com.au/~netsafe/trojan_index.html
DESC : Detailed information about windows trojans

URL : http://researchweb.watson.ibm.com/antivirus/SciPapers/Whalley/inwVB99.html
DESC : Windows trojans

URL : http://researchweb.watson.ibm.com/antivirus/SciPapers/Smoke/smoke.html
DESC : Another must read paper

URL : http://www.frame4.com/content/files/the_gentle_art_of_trojan_horsing_under_windows.txt
DESC : Windows trojans

URL : http://www.frame4.com/content/files/trojdetecte.txt
DESC : Snakebyte's tips about trojan detection

URL : http://www.frame4.com/content/files/what_trojan.pdf
DESC : Paper about windows trojans

URL : http://www.frame4.com/content/files/Trojan_reversing.txt
DESC : Interesting reading

-- Online Scanners --

URL : http://www.hackerwhacker.com/
DESC : A must visit vulnerability checker with unique features

URL : http://www.scannerx.com
DESC : Vulnerability assessment scanner

URL : http://scan.sygatetech.com/
DESC : Security scanner

-- Browser and E-mail Software --

URL : http://www.nwnetworks.com/iesc.html
DESC : Internet Explorer security centre

URL : http://www.guninski.com
DESC : Browser and active content researcher a must visit

URL : http://www.sophos.com/virusinfo/whitepapers/activecontent.html
DESC : Whitepaper about active content security

-- Misc --

URL : http://directory.google.com/Top/Computers/Security/Anti_Virus/Trojans/
DESC : Google's trojans directory

URL : http://support.microsoft.com/support/kb/articles/q262/6/31.asp?LN=EN-US&SD=gn&FR=0
DESC : Risky file extensions

URL : http://www.frame4.com/content/files/razor.wintrinoo.txt
DESC : Review of the WinTrinoo trojan

URL : http://www.megasecurity.org/Info/mIRC.txt
DESC : Very detailed paper on mIRC backdoors

20.Final Words

I really hope you've realised how big security problem Windows Trojan Horses are, and you've become
a little paranoid about your security. If you've ever found yourself infected, I also hope that while
reading the paper, you have understood how you may have gotten infected the last time and I'm sure you

won't make the same mistake again. The paper will be regularly updated with the latest info regarding the topic, as new variations of trojans and ways of infection appear very often. If you think I've missed something, please do not hesitate to contact me and contribute to it. Your feedback, ideas, comments, suggestions and everything related to the paper and the topic will be gratefully appreciated. I can be contacted at dancho.danchev@frame4.com.

Part of the Frame4 Security Systems Publications Archive, this paper can be located at http://www.frame4.com/publications/index.php. Please visit the archive to get the latest updates to this paper and many other security related documents.