

Trojans FAQ

FAQ topic

We have all heard alot about trojan horse programs and the threat that they pose to your network's security. This Trojan FAQ sheds some light on what these programs are, what they do, how they can infect your network and suggests measures that could be taken to prevent such infections. You can make sure that you have a good grasp on these malicious programs by browsing through this regularly updated Trojan FAQ which provides the answers to these questions and many others. With thanks to Dancho Danchev for his contributions to this FAQ.

FAQ: Part One - Introducing Trojans.

- 01.Introduction Last updated: **Jun 26, 2003**
- 02.What is a Trojan horse? Last updated: **Jun 26, 2003**
- 03.How do Trojans work? Last updated: **Jun 26, 2003**
- 04.What are their functions? Last updated: **Jun 26, 2003**
- 05.How dangerous are they? Last updated: **Jun 26, 2003**
- 06.What are the most common Trojans? Last updated: **Jun 26, 2003**

FAQ: Part Two - How and Why?

- 07.In what ways could I be infected? Last updated: **Jun 26, 2003**
- 08.How am I endangering my company's data once infected? Last updated: **Jun 26, 2003**
- 09.Why would they target me, or my company? Last updated: **Jun 26, 2003**

FAQ: Part Three - Protection and Response.

- 10.Do Anti-Virus Scanners provide reasonable protection? Last updated: **Jun 26, 2003**
- 11.Are there any effective Anti-Trojan Packages? Last updated: **Jun 26, 2003**
- 12.How do I know whether I have been infected? Last updated: **Jun 26, 2003**
- 13.What should I do once infected? Last updated: **Jun 26, 2003**

FAQ: Part Four - More Information.

- 14.Are there any other quality papers concerning the Windows Trojans subject? Last updated: **Jun 26, 2003**

- 15.Are there any recommended resources regarding further information on the topic?

Last updated: **Jun 26, 2003**

FAQ: Part Five - Policies and Prevention.

- 16.Can you provide me with tips in order to protect myself, as well as prevent possible infections?
- 17.How should we deal with potential malware problems in our company?
- 18.How should we deal with the dangers of Free E-mail providers, as far as protecting against Malware is concerned?

Last updated: **Jun 26, 2003**

Last updated: **Jun 26, 2003**

Last updated: **Jun 26, 2003**

FAQ: Part One - Introducing Trojans.

01.Introduction

Date - Jun 26, 2003 Author - Admin

Trojan Horses pose one of the most significant threats to the Windows OS, thus exposing sensitive information to malicious attackers, as well as providing them with full access to the computer, which often results in further illegal activities done via the infected computer. This paper will cover the Windows Trojans topic in-depth, it will highlight a lot of the important aspects, but will also act as a FAQ, summarizing the topic in a brief, easy to understand, yet effective and informative way. The FAQ will be updated on a monthly basis, so be sure to come back, although we've created a Newsletter for your convenience that will let you know when the site is being updated. [Subscribe Here](#).

[\[back top\]](#)

02.What is a Trojan horse?

Date - Jun 26, 2003 Author - Admin

Basically a Trojan horse can be defined as:

- o An unauthorized program contained within a legitimate program. This unauthorized program performs functions unknown (and probably unwanted) by the user.
- o A legitimate program that has been altered by the placement of unauthorized code within it; this code performs functions unknown (and probably unwanted) by the user.
- o Any program that appears to perform a desirable and necessary function but (because of unauthorized code within it that is unknown to the user) performs functions unknown (and definitely unwanted) by the user.

The trojan has borrowed it's name from the old mythical story about how the Greeks gave their enemy a huge wooden horse as a gift, but after the enemy accepted it, during the night the Greek soldiers crept out of the horse and conquered the city.

[\[back top\]](#)

03.How do Trojans work?

Date - Jun 26, 2003 Author - Admin

Most trojans come in two parts, a Client, and a Server, but there are exceptions where the trojan does not need a Client, as it's able to automatically do what it was intended to do (stealing passwords, business data etc.), without any intervention from the attacker. However those who use both Client and Server in order to operate need assistance from the attacker. Once the victim runs the Server (unknowingly), the attacker will use a port to connect to the Server (your computer) and start using the Trojan.TCP/IP is the usual protocol used, but there are exceptions using ICMP, and UDP as well. When the Server is executed on the victim's machine, it will hide itself somewhere within the computer and start listening on the specified by the attacker port. However there are trojans that automatically listen for incoming connections once run, which will wait a period of time to reduce the risk of being detected.

It's necessary for the attacker to know the victim's IP address to connect to his/her machine. Many trojans have features such as the ability to mail the victim's IP, as well as the ability to message the attacker via ICQ or IRC. This is used when the victim has a dynamic IP, which means that 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 in order to auto-run each time your computer is started. These methods include, but are not limited to, using the Windows Registry, using some of the Windows's System Files, as well as using third party configuration files.

System files are located in the Windows Directory. Here is a brief explanation of most of the common auto-starting methods that use the Windows System Files:

- o **Autostart Folder**

The Autostart folder is located in C:\Windows\Start Menu\Programs\startup and as its name suggests, automatically starts everything placed within this folder.

- o **Win.ini**

Windows system file using load=Trojan.exe and run=Trojan.exe to execute the Trojan.

- o **System.ini**

Using Shell=Explorer.exe trojan.exe results in execution of every file after Explorer.exe

- o **Wininit.ini**

Mostly used by Setup-Programs. Once it is run, it is auto-deleted, which is very handy for trojans to restart.

- o **Winstart.bat**

Acting as a normal bat file, the trojan is added as @trojan.exe to hide its execution from the user.

- o **Autoexec.bat**

It's a DOS auto-starting file and it's used as an auto-starting method like this -> c:\Trojan.exe

- o **Config.sys**

Could also be used as an auto-starting method for trojans

- o **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.

Windows Registry is another commonly used place regarding the auto-starting methods of the Trojans. 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 when ICQ detects an 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\InstalledComponents\KeyName]  
StubPath=C:\directory\Trojan.exe
```

All of the aforementioned methods are well known to the community, although you should not rely on them (by checking these Registry Entries, as well as the System Files ones) as a foolproof method for detecting Trojans, because new methods are discovered literally every day.

[\[back top\]](#)

04.What are their functions?

Date - Jun 26, 2003 Author - Admin

Windows Trojans vary in their functions and abilities, although here's a brief summary of the most common ones:

- Change the victim's resolution. This function displays a list with all the resolutions available on the victim's computer and the attacker just pick one and hit "change it!", after that you'll have your resolution changed
- Notify. The attacker is notified by e-mail, ICQ, IRC when you're online, as well as your IP if you have a dynamic one
- Processes monitoring. The attacker has the ability to monitor all of your processes, start new ones, as well as the ability to kill current one.
- Registry editor. It gives to the attacker, the ability to view/create/delete/change everything in the registry.
- Find files feature. Provides the attacker with the opportunity to find any file on the hard drive, if he/she is looking for something particular.
- ScrollLock, CapsLock, NumLock can be turned ON and OFF by the attacker, this function is defined as a "fun" one.
- Disconnect victim. The attacker can hang up the victim's connection to the net at anytime.
- Screenshot. The attacker can make screenshots of your activities, which are directly transferred to his/her computer, however there are more advanced functions including Web Cam monitoring, as well as microphone recording, if you have any of these of course.
- Flip Screen. That's an obvious one, and it's again considered as a "fun" one
- Hide/Show the victim's desktop icons. Annoying the victim is what amuses people sometimes.
- FTP server. This option turns your PC into a FTP server accessible by the whole world, or to the attacker only.
- Open the browser at an address specified by the attacker.
- Hide/show the Start button.
- Enable/Disable keyboard.
- Chat with the victim. Interesting function enabling the attacker to open an ICQ look-alike chat with the victim.

- Start/stop the victim's PC Speaker.
- Restart windows.
- Open/Close the CD-ROM tray.
- Turn monitor on/off.
- Get more information about the victim's computer. For example: windows version, user name, company name, screen resolution, etc.
- File manager. This function acts as an explorer for the attacker while browsing through your system.
- Retrieve passwords. This function will provide the attacker with the recorded passwords on your computer.
- KeyLogger. Logs all of the keys you've pressed, could be achieved in offline/online mode.

There you have the most common Trojan's functions. As you've noticed most of these could be, and are, pretty dangerous and destructive ones.

[\[back top\]](#)

05.How dangerous are they?

Date - Jun 26, 2003 Author - Admin

Windows Trojans represent a large security threat to your computer. Here I'll cover various scenarios, as well as provide you with further information so that you'll be able to realize how dangerous they are indeed.

As you've noticed while reading all of the aforementioned functions, they can be pretty dangerous. The attacker can have access to ALL of your files, personal information, sensitive work projects, and other confidential information just using the Keylogger, and the Explorer functions. In most cases the attacker will be looking for:

- 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?!).
- Schoolwork (steal your papers and publish them with his/her name on it).

You should realize that Trojans can be very destructive, and that they're not only used to delete files, but to steal people's work, job projects, and many other illegal activities.

On the other hand some advanced attackers will use your computer in order to commit further online crimes, and involve you in other illegal activities, thus turning your computer into a proxy, enabling them to move through your computer without any traces left, before they reach their potential aim. It can be illustrated as:

attacker--->your computer--->computer to be attacked

(turned into a proxy)

As you can see this is extremely dangerous to you, as the traces will lead back to you, no matter what is the attacker doing while having access to your PC, in 99% of the cases it will be an illegal activity.

You can contribute to a DDoS (Distributed Denial Of Service Attack), as your computer might be turned into the so called "zombie", proving the attacker with the ability to use your bandwidth for flooding and causing damage to other networks.

[\[back top\]](#)

06.What are the most common Trojans?

Date - Jun 26, 2003 Author - Admin

Here are the most popular kinds, although most of these represent a combination of several more, and let's not forget the non-public ones, which will never be released to the public, and are used for the attacker's illegal activities, those are some of the most dangerous ones.

Remote Access Trojans (RAT's)

These are probably the most publicly used Trojans, simply because they give the attackers the power to do more things on the victim's machine than the victim himself, while standing in front of the machine. The idea of these Trojans is to give the attacker 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 cached passwords and also look for other passwords you're entering, then sends 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.

Keyloggers

These trojans are very simple. The only 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 such as 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.

Denial Of Service (DoS) Attack Trojans

These trojans are becoming very popular these days, giving the attacker the power to start a

DDoS if having infected 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 happened 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

An interesting feature implemented in many trojans is the ability to turn the victim's computer into a proxy/wingate server available to the whole world or only to the attacker. 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 simplest ones and are kind of outdated as the only thing they do is open port 21(the port for FTP transfers) and let EVERYONE connect to your machine or only 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, enabling the attacker 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.

[\[back top\]](#)

FAQ: Part Two - How and Why?

07. In what ways could I be infected?

Date - Jun 26, 2003 Author - Admin

The Complete Windows Trojans Paper discusses in-depth each of the possible scenarios as far as becoming infected with a trojan is concerned. You're strongly advised to closely look at them, thus being able to understand and properly react to the threat posed by the Windows

Trojans.

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 whom 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 is it to launch such attacks with only the click of 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 that particular moment. It could be someone that hacked your friend's ICQ UIN (Unique Identification Number) and wants to spread some trojans among 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, which creates a site on your computer, with your info from the ICQ database. The bug constitutes a security hole 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 realize 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 Trojan....(150 spaces).txt.exe, icon changed to a real .txt file and this will definitely get you infected. This bug has almost certainly been fixed in the newer version.

No matter which Instant Messenger Application you're using, you could always get yourself infected by certain program bugs that you have never had the chance to hear about, and never took the precaution of checking for newer versions of the application. Also when you're receiving files no matter where and no matter from whom, take this potential threat very seriously and recognize the dangers of naive behavior.

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, whether they are pretending to be free porn archive, whether offering software for "free internet" or offering a Hotmail hacking program, DO NOT download any of these files. Newbies are often targets of these fakes, and believe me, many people are still newbies where security is concerned. Users get infected from porn-trade channels, and of course, warez channels, as they don't think about the risk but think only of getting free porn and free programs instead.

Here are several scenarios of how you may become infected while using IRC:

- You're talking with someone, probably a "girl", having 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 and offers it to you, but how about if "she" mentions several pictures are nude 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 nude and she hasn't lied 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 Trojan....(150 spaces).txt.exe you'll get the file over IRC and in the DCC it will appear as .TXT and as a result you won't become suspicious, 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 really is a text file.

Via Attachments

I'm always amazed by the number of people that get themselves infected by an attachment sent to their mailboxes. Most of these users are new to the Internet and are pretty naive. When they receive an email containing an attachment saying that they will get free porn, free Internet access etc., they run it without completely understanding the risk to 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 as to what it is all about, and when he finishes coding the application you wait for an e-mail from him with the attachment. 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 has his program ready and has sent it as an attachment. 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 in this way you've just been infected.

Information Is Power! Simply because the attacker knew you were waiting for some particular file, he went ahead and found Alex's e-mail address and infected you...the timing of the attack 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 actually came from some .jp mail server relaying e-mails and has been used by spammers for several months.

Many people have gotten themselves infected by the famous "Microsoft Internet Explorer Update" sent directly to their mailboxes, by the nonexistent Microsoft Updates Staff. I understand you may have felt great because Microsoft were paying you special attention and sent you the latest updates, but these "updates" are definitely trojans. Microsoft will NEVER send you updates of their software via e-mail even if you see that the FROM field is updates@microsoft.com and as you've noticed in the previous example the FROM field could be 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 an extremely dangerous problem that requires you to keep yourself constantly up-to-date with the latest version of any software you're using.

Physical Access

Physical access is vital for your computer's security. Imagine what an attacker could do while having physical access on your machine, and let's not forget to mention that if you're always connected to the Internet and leave the room for several minutes that you've just given long enough of a chance to get yourself infected. Here I'll illustrate 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 gaining 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 his/her 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 in order to accomplish their 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 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 similar to the previous ones might be a sudden ring of the doorbell, 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 comes to your sensitive computer data.
- Another method of infecting a computer while having physical access is through use of 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 since most of you probably aren't aware of this CD function, you will become infected and won't understand what has happened and how it has 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 think 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 has 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 available in IRC whose only function is 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 a specific software such as a new version of some program infected with a trojan of course, and visits some URL known only to him/her and then downloads 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 simply downloads and executes the file, hereby infecting the computer. In this case the mail service is used as a storage area.

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 the activities that I have mentioned here. After that, the attacker will be able to choose the best variant for infecting the victim and doing the job.

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 having downloaded or executed any programs. The same scenario occurs when you check your E-mail with Outlook Express or some other software with well known problems. Again you will be infected without having downloaded the attachment. Make sure that you always have the latest version of your Browser and E-mail Software, thus reducing the risk to a minimum.

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 Win ME, 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.

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 than 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 probably using it every day because it's working very well, no problems ever occurred, you're happy, but a lot of things are going on 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. 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 into trusting it. Pay attention to freeware tools that you download, regard them as extremely dangerous and as a very useful and easy way for attackers to infect your machine with a Trojan.

Freeware Software, and the so called "Hackers" Web Sites

A site located at some free web space provider or just offering some programs for illegal activities can be considered as an 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 filled with "hacking" programs, scanners, mail-bombers, flooders and many other tools. The guy who created the site infects often several, if not all of these programs. 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 that risk? There are some untrusted sites that look REALLY professional and boast huge archives full of Internet related software, feedback forms and links to other popular sites. I think if you take some time, look deeper, scan all the files you download, then you can decide on your own whether the site you are downloading your software from is a trusted or an untrusted one. Freeware programs should 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 a 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 minimized. If no reviews or comments about the software are found via the search engines, then it may be highly risky to start using it.

[\[back top\]](#)

08.How am I endangering my company's data once infected?

Date - Jun 26, 2003 Author - Admin

Once infected, critical business data could be exposed to a malicious attacker or a corporate spy. You should not assume that the data is properly protected by the company's firewall, and that even if you get infected, that there would be no way for the attacker to get the data. Firewalls are essential and will block their attempts to connect to the Server (your computer), however attackers are becoming more creative and adaptive, so there are ways to retrieve the

data without the need to connect to your computer. You can also unknowingly participate in exposing the whole network to attack, there at work, just by having your computer infected with a Trojan Horse.

[\[back top\]](#)

09. Why would they target me, or my company?

Date - Jun 26, 2003 Author - Admin

In fact most of the times no one is targeting you in particular, it's just your bandwidth and the access to your computer that they're trying to get to. However there is the possibility that someone wants to attack you or your company in order to obtain classified business or sensitive personal data.

[\[back top\]](#)

FAQ: Part Three - Protection and Response.

10. Do Anti-Virus Scanners provide reasonable protection?

Date - Jun 26, 2003 Author - Admin

You must realize that there isn't a 100% sure way of protecting against Windows Trojans infections, although your major aim is to significantly reduce the risk by understanding how they work and how you could become infected.

This type of software relies mainly on the "signatures" that each trojan executable has and also it's common auto-starting methods. But this is not a perfect solution by far for protecting 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 first 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 to attract new users. As a result, most of them became really advanced trojan scanning and detection systems, but for maximum protection it's recommended to use both Anti-Virus and Anti-Trojans software. Public trojans appear online almost every day and detection software is being updated every day to provide its customers with maximum protection. 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 of the latest 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 for any reason, do **NOT** run it, but send it to your detection software labs for analysis.

[\[back top\]](#)

11. Are there any effective Anti-Trojan Packages?

Date - Jun 26, 2003 Author - Admin

Yes, there are, although you should never fully rely on them as they only partly solve the problem. It's you who has the responsibility of maintaining an acceptable level of protection. While these Packages should be used on standalone computers or very small networks, it is recommended that companies use Gateway protection Packages if they seek an improvement in their security by limiting the dangers posed by their Internet connectivity.

Here are links for some of the popular Anti-Trojan Packages that should be used in the company's Defense In Depth methodology, whose main purpose is to put another line of Security by protecting the end users workstations.

Enduser Protection Packages

- **TDS-3**

Trojan Defense Suite (TDS) is an 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/>

- **Tauscan**

Trojan scanner that has unique features and is a must have. It's also able to detect new trojans and trojans that have never been released to the public. More info at its official page: <http://www.agnitum.com/products/tauscan/>

- **Trojan Hunter**

Trojan detection package with a lot of functions. It's very handy. More info at <http://www.mischel.dhs.org/trojanhunter.jsp>

Gateway Protection Packages

- **GFI MailSecurity** - [More Info](#)
- **McAfee Internet Gateway Protection** - [More Info](#)
- **TrendMicro's Internet Gateway** - [More Info](#)
- **Symantec AntiVirus Gateway Solution** - [More Info](#)
- **Symantec AntiVirus for SMTP Gateways** - [More Info](#)

Free Online Trojan Scanning

- **GFI TrojanScan** - [More Info](#)

[\[back top\]](#)

12. How do I know whether I have been infected?

Date - Jun 26, 2003 Author - Admin

The most common trojans features have been listed above, so that by knowing them you'll be able to detect suspicious activities going around your computer. However you should keep in mind that advanced attackers will keep as silent as possible, in order to continue their illegal actions on your computer. The following events should be considered as a suspicious one:

- It's normal to visit a web site and several more pop-ups appear with the page you've visited. But alternatively, suddenly your browser directs you to some page unknown to you without you having done anything at all. Take that as a serious indication of infection.
- 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.
- You doing absolutely nothing, no Internet related applications are running, but your modem lights are going crazy, just the way they are when you're downloading files or actively using the Internet. Consider this as an extremely suspicious sign.

GFI Software has released the GFI Trojan scanning service, which is another highly recommended way to scan your computer for Trojans. Access the service [here](#).

[\[back top\]](#)

13. What should I do once infected?

Date - Jun 26, 2003 Author - Admin

- 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 a connection. Immediately change your ICQ, mIRC passwords if they're still the same. (Often attackers won't change any of your logins and passwords to fool you into thinking that everything is OK, so there is a good chance that you will still be able to recover from the compromise). Change your web based e-mail passwords and do check your information that is stored there, because 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 the e-mail addresses of friends, colleagues, etc. there is a real possibility that the attacker has sent them a trojan and has possibly infected them too. Mail all of these people and ask them about whether they have received any files from your mailbox, inform them someone else might know your e-mail password so that they'll be able to take appropriate actions such as 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 have mentioned, kiddie-porn archives.
- Think for a while about the sensitive information you have had on your machine before

the compromise, and if you are absolutely certain that the attacker may now possess this information, then take appropriate action, such as informing any institutions that own the sensitive data that a breach has occurred.

- 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 despite the fact that the attacker no longer has access to your machine.
- Monitor your processes BEFORE and AFTER connecting to the Internet, as some trojans start when they detect Internet connection. Don't be fooled again, be very suspicious.

[\[back top\]](#)

FAQ: Part Four - More Information.

14. Are there any other quality papers concerning the Windows Trojans subject?

Date - Jun 26, 2003 Author - Admin

Yes, there are. Follow the links below:

- http://secinf.net/trojans/The_Complete_Windows_Trojans_Paper.html
- <http://www.jmu.edu/computing/info-security/engineering/issues/remote.shtml>
- http://members.ozemail.com.au/~netsafe/trojan_index.html
- <http://researchweb.watson.ibm.com/antivirus/SciPapers/Whalley/inwVB99.html>
- <http://researchweb.watson.ibm.com/antivirus/SciPapers/Smoke/smoke.html>
- http://www.frame4.com/content/files/the_gentle_art_of_trojan_horsing_under_windows.txt
- http://www.frame4.com/content/files/what_trojan.pdf

[\[back top\]](#)

15. Are there any recommended resources regarding further information on the topic?

Date - Jun 26, 2003 Author - Admin

Windows Trojans pose a significant threat to the security of your computer; hence the Internet is filled with sites that discuss the topic. Follow the links below:

- <http://www.tlsecurity.net>
- <http://www.megasecurity.org>
- <http://www.trojan.ch>
- <http://www.trojanforge.net/>
- <http://packetstormsecurity.org/trojans>
- <http://www.pcflank.com>

Packages Review Web Sites:

- <http://www.anti-trojan-software-reviews.com/>
- <http://www.staff.uiuc.edu/~ehowes/trojans/tr-tests.htm>
- http://www.wilders.org/anti_trojans.htm
- <http://www.firewallguide.com/anti-trojan.htm>

[\[back top\]](#)

FAQ: Part Five - Policies and Prevention.

16. Can you provide me with tips in order to protect myself, as well as prevent possible infections?

Date - Jun 26, 2003 Author - Admin

Here's a summary of the whole FAQ. You'll learn how to behave in a secure manner while reading these tips, and don't forget that they could be a lifesaver as far as Windows Trojan threats are concerned.

- Never accept a file even it is from some friend. You're never absolutely sure who's on the other side of the computer at any given moment. If you really need this file, let's say it's some presentation or a work paper, find other ways such as by telephone and verify that the file is indeed from your friend. Yeah it will take you some time and slow you down a bit, but by being paranoid about the attachments you may receive you won't get infected in this way.
- When executing files, first check their type. Is it really a .doc or it's some executable with a .doc icon?
- Update your Anti-Virus and Anti-Trojan package signature files regularly, if possible EVERY day for maximum 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 maximum protection.
- 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 that have been found in the software that may potentially put your system at risk - and patch/update your system(s) accordingly. Some software has an option to check for the latest version of the software from the vendor's web site; make use of it.
- Take several minutes and regularly check the processes on your machine with the software I have reviewed above. You'll be surprised at what you may detect sometimes.
- It's vital to understand the risk of getting software from someone you have just met, or from someone that you have only had several ICQ, IRC conversations with.
- Consider freeware programs as very risky software to download, and try searching for some reviews of the program before running it.
- Carefully read the help files that come with your detection software in order to be able to use them to their full capacity.
- Download software ONLY from its official page(s) or dedicated mirror web site. Never get the latest version of mIRC, ICQ or from some site you've never heard about such as

from some free web space provider like Geocities. Consider it as an untrusted site and do NOT download anything from there.

- o 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.
- o Don't be so naive in regards to everything that you see on the Internet or in regards to what various sites offer you don't download any software you've never heard about.

[\[back top\]](#)

17.How should we deal with potential malware problems in our company?

Date - Jun 26, 2003

Author - Admin

Security Policy

First of all you should establish an Anti-Malware Policy, guiding the staff members on the process of protecting critical company data from destruction or exposure. It needs to clearly state their responsibilities while using any of the company's Information Resources, thus making sure that it will be easily understood and properly implemented later. You should define what is allowable and what is not, what they should and what they shouldn't do in order to keep their workstations, as well as the company's network free of malware. Keep it short, precise and easy to understand, know your audience before your start building it, measure their computer/security level skills for maximal effectiveness. A sample Anti-Virus Policy can be found [here](#).

Gateway Protection

You might consider using Gateway Protection, detecting and blocking malware at the Server level before reaching the workstations. A few reasonable products for this activity are:

- o Symantec AntiVirus Gateway Solution - [More Info](#)
- o Symantec AntiVirus for SMTP Gateways - [More Info](#)
- o Symantec Anti-Virus Corporate Edition - [More Info](#)
- o GFI MailSecurity - [More Info](#)
- o GFI DownloadSecurity - [More Info](#)

Content Blocking

Another valuable strategy that might be implemented, in the company's effort to protect its critical data from malware, is to filter known to be dangerous and potentially destructive file extensions at the Server level. These include: .exe, .com, .vbs, .scr, .asd, .asf, .asx, .bas, .bat, .chm, cmd, .com, .dll, .exe, .hlp, .hta, .hto, .js, .jse, .link, .lnk, .pif, .reg, .scr, .vb, .vbe, .vbs, .wsf, .wsh, and .wsc. A list of dangerous extensions may be found [here](#).

Whenever someone from the company needs to receive a specific attachment having one of these extensions, the receiver might ask the sender to change the file's extension, and in this way confirms that indeed, a known person has sent the attachment.

[\[back top\]](#)

18.How should we deal with the dangers of Free E-mail providers, as far as protecting against Malware is concerned?

Date - Jun 26, 2003 Author - Admin

In your Anti-Malware Policy, you need to state whether the use of Free E-mail providers is allowed or it is strictly prohibited. Educate them on the problem of potentially destructive attachments, downloaded from their external e-mail and run on the company's network. On the other hand, if the use of these services is prohibited due to security policy, then block access to these and let your staff members know that the proper use of the E-mail system is being strictly monitored.

[\[back top\]](#)

We have all heard alot about trojan horse programs and the threat that they pose to your network's security. This Trojan FAQ sheds some light on what these programs are, what they do, how they can infect your network and suggests measures that could be taken to prevent such infections. You can make sure that you have a good grasp on these malicious programs by browsing through this regularly updated Trojan FAQ which provides the answers to these questions and many others. With thanks to Dancho Danchev for his contributions to this FAQ.