Norton
from symantec

# Malware Removal Guide

**The NortonLive Team**

February
2010

## *IMPORTANT NOICE*

BEFORE YOU USE THIS DOCUMENT FOR SELF-HELP SUPPORT, PLEASE READ THE TERMS BELOW CAREFULLY. IF YOU DO NOT AGREE TO THE TERMS, THEN SYMANTEC IS UNWILLING TO PROVIDE THE INFORMATION CONTAINED IN THIS DOCUMENT TO YOU, IN WHICH CASE YOU SHOULD NOT USE THIS DOCUMENT OR CONDUCT SELF-HELP SUPPORT. BY YOUR USE OF THIS DOCUMENT, YOU ARE DEEMED TO HAVE ACCEPTED AND CONSENTED TO BE BOUND BY THE TERMS BELOW.

ANY AND ALL INFORMATION AND/OR SOFTWARE IN THIS DOCUMENT ARE PROVIDED "AS IS" WITHOUT WARRANTY OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT.

SYMANTEC ASSUMES NO RESPONSIBILITY FOR ERRORS OR OMISSIONS IN THE INFORMATION OR SOFTWARE WHICH ARE REFERENCED BY THIS DOCUMENT. IT IS SOLELY YOUR RESPONSIBILITY TO COMPLETE A BACKUP OF ALL EXISTING DATA, SOFTWARE, AND PROGRAMS BEFORE USING THIS DOCUMENT(INCLUDING SELF-SUPPORT) OR PERFORMING ANY TASKS REFERENCED IN THIS DOCUMENT.

IN NO EVENT SHALL SYMANTEC BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT OR CONSEQUENTIAL DAMAGES OF ANY KIND, OR ANY DAMAGES WHATSOEVER (INCLUDING WITHOUT LIMITATION, THOSE RESULTING FROM: (1) RELIANCE ON THE MATERIALS PRESENTED, (2) COSTS OF REPLACEMENT GOODS, (3) LOSS OF USE, DATA OR PROFITS, (4) DELAYS OR BUSINESS INTERRUPTIONS, (5) AND ANY THEORY OF LIABILITY, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF INFORMATION) WHETHER OR NOT SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SOME STATES AND COUNTRIES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THE ABOVE LIMITATIONS OR EXCLUSIONS MAY NOT APPLY TO YOU.

THIS DOCUMENT COULD INCLUDE TECHNICAL OR OTHER INACCURACIES. CHANGES ARE PERIODICALLY MADE TO THE INFORMATION HEREIN. HOWEVER, SYMANTEC MAKES NO COMMITMENT TO UPDATE MATERIALS ON THIS DOCUMENT.

# *Introduction*

Currently there are thousands of new computer viruses or other types of malware discovered each month. Many of these threats are designed to resist detection, and removal, and may disable the execution of your antivirus software, and your computer's ability to connect to online scanning that can provide remediation. Still other threats reinstall themselves almost as quickly as they are removed.

As threats to our personal information and computer systems grow, so do our tools to attempt to fight them. Unfortunately it is not always possible to be prepared for every threat. In those cases where infection occurs due to out-of-date virus definitions or not yet patched system code, and the threat has latched onto a system and current antimalware solutions are not yet able to remediate the situation, a manual virus removal solution is called for.

For those interested in pursuing the removal yourself, we offer a Do-It-Yourself guide for manual virus and malware removal. If you need professional assistance to detect and remediate your infected computer, please feel free to contact our NortonLive Spyware & Virus Removal service experts at 1(877) 788-4877, or visit:
http://www.symantec.com/norton/support/premium_services/premium_virus.jsp

> **Note:** Some of the following steps may require an advanced understanding of the Windows Operating System; we highly suggest having a skilled technician perform virus removal if you believe you are at risk. Be sure to back up your system before attempting to remove a virus. Failure to do so may result in your computer becoming unresponsive, and permitting data loss.

The suggestions in this article are not intended to 100% guarantee removal of all threats from a compromised PC. The process may also take a number of hours and several iterations to detect and remove suspicious threats, and may render your PC unusable.

Effective malware removal requires a good deal of preparation. A few things to have handy would be your:

- Operating System or Reinstall disks.
- Malware Removal Product installation disc
- Latest updated virus definitions.

- A current backup of your important files.
- Set a System Restore Point

Do not attempt to perform malware removal without first backing up your important files and folders.

It is recommended that you read through this document in its entirety before attempting remediation of your virus issues. When you are ready to attempt removal, a Table of Contents has been added so that you can quickly jump to a particular section for easy reference.

## Contents

Introduction ..... 3

Threat Types ..... 9

Viruses: ..... 9

File Infector ..... 9

Boot Sector Infector ..... 9

Multipartite Virus ..... 10

Macro Virus ..... 10

Polymorphic Virus ..... 10

Metamorphic Virus ..... 10

Worms: ..... 10

Trojan horses: ..... 11

Spyware: ..... 11

Rogue Antispyware: ..... 11

Adware ..... 12

Rootkits ..... 12

User Mode Rootkits ..... 12

Kernel Mode Rootkits ..... 13

DNS Poisoning ..... 13

Removal Process ..... 14

Identification ..... 14

Process Analysis ..... 15

Common Load Points: ..... 16

THE WININIT.INI FILE ..... 19
Other load points ..... 19
Startup Folders: ..... 20
File System ..... 21
Network Analysis ..... 22
Troubleshooting Network Connectivity ..... 22
Check your Network Status ..... 22
Using the Ping Command ..... 23
Verify your Internet Protocol address ..... 24
Browser Hijacking and Redirects ..... 24
Examine your Hosts file ..... 24
Using the Netstat Command ..... 25
Port Types ..... 26
Well Known Ports ..... 27
Registered Ports ..... 27
Dynamic/Private Ports ..... 27
Boot Analysis ..... 27
Internet Browser ..... 28
Browser Helper Object (BHO) ..... 28
Add-ons ..... 28
Home Page and Default Search ..... 29
Safe Mode ..... 30
Removal ..... 30

Verification ..... 31
Final Cleanup ..... 31
Clean your Recycle Bin ..... 31
Purge your Temp Folders ..... 31
Update your Virus Definitions ..... 32
Ensure Windows Updates ..... 32
Reset System Restore ..... 33
Set Restore Point ..... 34
Reset File Views ..... 35
Restore UAC (Microsoft Vista & Windows 7) ..... 35
Virus Removal Examples ..... 36
Infostealer.Banker.C ..... 36
Trojan.DNSChanger-Symantec ..... 38
OS Considerations ..... 41
XP ..... 41
Vista ..... 41
Win7 ..... 42
64-bit Operating Systems ..... 42
Professional Assistance ..... 43
Additional Information ..... 43
Introduction to Safe Computing ..... 43
Install and Use an Anti-Virus Program ..... 44
Patch the Operating System ..... 44

Handle Emails with Care ..... 45
Social Engineering Attacks: ..... 45
Install a Firewall ..... 46
Backup files periodically ..... 47
Use (strong) Passwords ..... 48
Appendix ..... 51
Ports Commonly Used by Trojans ..... 51

# *Threat Types*

Threats to your computer system, data, and identity come in many different forms, a few of the most common are listed as follows:

## *Viruses:*

A virus is a self-replicating program that is designed to damage or degrade the performance of a computer. A virus is replicated by being copied or by initiating its copying to another program, computer boot sector or document. Viruses can be classified into four different categories as follows:

- File Infector
- Boot Sector Infector
- Multi-partite
- Macro virus

**File Infector**

A File infector virus when executed on a system will seek out other files and insert its code into them. The programs with .EXE and .COM extensions are the most commonly targeted, but a file infector virus can target any executable file. When the application is started, the infection is executed and carries out its designated task. It is commonly injected into the system memory. There it waits for a trigger from which to corrupt other items. This infection is most commonly distributed via compromised networks, over the web via drive-by, or from a corrupted media (CDRW, flash media). One of the most prevalent forms of the file infector contains a variant of the Win32 virus. Its purpose is to transfer hits to the HttpSendRequest into a corrupted .DLL format. This type of file infector is often installed by other malware. The file infector employs a technique to make sure its corrupted .DLL format will replace the targeted extensions found within the system. When the computer is rebooted, it incidentally boots the infected file and continues its advancement throughout the system.

**Boot Sector Infector**

A Boot Sector infector is a virus that infects the leading sector of a hard drive or other bootable media. Many boot sector infectors have the ability to modify the volume label of the storage drive. It may be transferred as a result of a pirated software application. Though less common today than in the past, this type of virus

was capable of causing considerable damage, as most operating systems will attempt to boot a computer from the first sector of the boot drive.

**Multipartite Virus**

A Multipartite Virus is a virus that infects and spreads in more than one way. The term was derived from the discovery of a virus that contained both a boot sector infector, as well as a file infector attack. To fully remove the threat, all parts of the virus must be removed. Due to the multiple vector for the spread of infection, these virus could spread faster than a boot or file infector alone.

**Macro Virus**

A Macro Virus is a virus that is written in a language specific to a software application such as a word processor. Since some applications (such as parts of Microsoft Office) allow macro programs to be embedded into documents, this allows the virus to run automatically when the document is opened, a distinct mechanism is provided by which the virus can be spread. Certain encryption techniques can make the detection of this threat beyond the scope of many antivirus programs.

Since a macro virus depends on the application rather than the operating system, it can infect a computer running any operating system of which the targeted application is running on. A macro virus infection can be avoided by exercising caution when opening email attachments and other documents.

**Polymorphic Virus**

A Polymorphic engine is used to create a virus that can be programmed to mutate itself with each infection, making detection more difficult. This type of malware infects with an encrypted copy of itself, and the decryption module is modified on each infection.

**Metamorphic Virus**

Using a Metamorphic engine, some virus's can rewrite themselves completely on each new execution. This helps the virus avoid being detected by emulation. These types of virus's are typically extremely large.

## *Worms:*

Worms are programs that replicate themselves from system to system without the use of a host file. In contrast, viruses which require the spreading of an infected host file. The most common way for a worm to propagate is to copy itself to outbound email as a file

attachment or transfer itself across a network through open network shares. Once a worm is on the system, it does not have to be executed by the user. It is important to note that some Worms will drop Trojan Horses on a customer's machine to open a network port for communication with a third party.

## *Trojan horses:*

Trojan horses are impostors, files that claim to be something desirable but, in fact, are malicious. A very important distinction from true viruses is that they do not replicate themselves. Trojans contain malicious code that, when triggered, cause loss or even theft, of data. For a Trojan horse to spread it must be invited onto your computer. A Trojan horse does not have reproduction capability and can only be executed by the user. Once a Trojan horse is executed, it delivers its payload. The payloads differ but most of the recently created Trojans are designed to steal passwords or open a port for communication.

## *Spyware:*

Spyware is a generic term for a class of software designed to either gather information for marketing purposes or to deliver advertisements to Web pages. A spyware aids in gathering information about a person or organization without their knowledge, and can relay this information back to an unauthorized third party. Because spyware is not viral, anti-virus software does not offer protection. By attaching itself to legitimate downloads, spyware easily passes through firewalls unchallenged. By intertwining itself with files essential to system operation, spyware cannot safely be removed by simply deleting files with a system cleaning tool.

## *Rogue Antispyware:*

Rogue/Suspect implies that these products are of unknown, questionable, or dubious value as antispyware protection. These products do not provide proven, reliable anti-spyware protection and may be prone to exaggerated false positives. Others may use unfair, deceptive, high pressure sales tactics to pressure sales from gullible, confused users. A few of these products are either associated with known distributors of spyware/adware or have been known to install spyware/adware themselves. Rogue antispyware is difficult to define as the intentions of the group vary. Typically members of the group claim to be a legitimate anti-spyware application but are in fact nothing more than an inexpensive clone of unreliable software. Rogues are often repackaged and given new names. Others among this group present false positives due to bugs in the software's code, not because of an outright lie. Code corrections can move a suspected rogue off of detection lists. Many rogue applications use deceptive or high-pressure sales tactics to convince users into buying a license. Users will be told that they need to buy protection even if there is nothing

dangerous found. Free scans are offered but a license is needed before any dangers can be removed. Free, fully functional trial periods are usually not offered. Spyware or other malware sometimes silently installs rogue antispyware that then offers to remove the spyware. Trojans and toolbars are other sources prompting for rouges to be installed. Affiliate marketing programs are often used to sell rogue antispyware.

## *Adware*

Adware is a type of program that displays an advertisement of some sort, usually related to a specific website cached in the web browser. In some cases, it changes the home page of your web browser to point to a specific web site. Because adware is not malicious in nature, it is not considered a virus. Adware can do a number of different things to your system. It can monitor and profile your web usage and direct pop up ads based on your surfing habits. Most peer-to-peer file sharing programs come bundled with adware and the user is only notified of this in the fine print of the End User License Agreement. Adware is not as dangerous as other infections, but it can be incredibly annoying. These are the types of programs that download files onto your computer by saying they are necessary for certain websites to work or without notifying you at all. They can take up your computers resources and are largely responsible for the countless popup ads you receive on the web.

## *Rootkits*

Rootkits are specialized programs that exploit known vulnerabilities in an operating system. These programs are available in abundance on the Internet and are used by hackers to gain root (administrator level) access to a computer.

In Windows, two basic classes of Rootkits exist –user mode Rootkits and kernel mode Rootkits.

### **User Mode Rootkits**

A user mode rootkit involves system hacking in the user or application space. Whenever an application makes a system call, the execution of that system call follows a predetermined path and a Windows rootkit can hijack the system call at many points along that path.

One of the most common user mode techniques is the memory modification of system DLLs. Windows programs utilize common code found in Microsoft provided DLLs. At runtime, these DLLs are loaded into the application's memory space allowing the application to call and execute code in the DLL.

**Kernel Mode Rootkits**

A kernel mode rootkit involves system hacking or modification in the kernel space. Kernel space is generally off-limits to standard authorized (or unauthorized) users. One must have the appropriate rights in order to view or modify kernel memory. However, the kernel is an ideal place for system hacking because it is at the lowest level and thus, is the most reliable and robust method of hacking. The system call's path through the kernel passes through a variety of hook points. A few of these points will be described below.

As a system call's execution path leaves user mode and enters kernel mode, it must pass through a gate. The purpose of the gate is to ensure user mode code does not have general access to kernel mode space protecting the kernel space. This gate must be able to recognize the purpose of the incoming system call and initiate the execution of code inside the kernel space and then return results back to the incoming user mode system call. The gate is effectively a proxy between user mode and kernel mode. In older versions of Windows, this proxy is invoked through interrupts and in newer versions of Windows through Model Specific Registers (MSRs). Both mechanisms can be hooked causing the gate to direct execution to the rootkit rather than the original kernel mode code.

Another popular hook point is to modify the System Service Descriptor Table (SSDT). The SSDT is a function pointer table in kernel memory that holds all the addresses of the system call functions in kernel memory. By simply modifying this table, the rootkit can redirect execution to its code instead of the original system call. Similarly to the previously mentioned techniques, the rootkit would likely call the original system call and then remove itself from the results before passing back the results. Finally, another kernel mode rootkit technique is to simply modify the data structures in kernel memory. For example, kernel memory must keep a list of all running processes and a rootkit can simply remove themselves and other malicious processes they wish to hide from this list. This technique is known as direct kernel object modification (DKOM).

## *DNS Poisoning*

Typically a networked computer uses a Domain Name System (DNS) server to associate website names with IP addresses that a computer can use to negotiate a connection.

Poisoning attacks on a single DNS server can affect the users serviced directly by the compromised server or indirectly by its downstream server(s) if applicable.

To perform a cache poisoning attack, the attacker exploits a flaw in the DNS software. If the server does not correctly validate DNS responses to ensure that they are from an authoritative source, the server will end up caching the incorrect entries locally and serve them to other users that make the same request.

This technique can be used to direct users of a website to another site of the attacker's choosing. For example, an attacker spoofs the IP address DNS entries for a target website on a given DNS server, replacing them with the IP address of a server he controls. He then creates files on the server they control with names matching those on the target server. These files could contain malicious content, such as a computer worm or a computer virus. A user whose computer has referenced the poisoned DNS server would be tricked into accepting content coming from a non-authentic server and unknowingly download malicious content.

# *Removal Process*

The removal process involves several steps that may need to be repeated a number of times to facilitate remediation.

1. Identification
2. Safe Mode
3. Removal
4. Verification
5. Cleanup

## *Identification*

A first step in identification of an infection is to change your file folder viewing options.

In XP and older operating systems, to access the folder options settings, you can open **Folder Options** in the **Control Panel**, or, from a folder window by clicking **Tools**, and then **Folder Options**. In Vista and Windows 7 you can type **Folder Options** into the **Search Bar**.

Once you open the **Folder Options** window, select the **Advanced tab**, and under **Hidden Files and Folders** select **show hidden files, folders, and drives**. In addition to this uncheck the boxes next to **Hide extensions for known files types**, and **hide protected operating system files**. You will be presented with a warning but choose **yes** to continue anyway.

Just like any program, in order for the program to work, it must be started. Malware programs are no different in this respect and must be started in some fashion in order to do what they were designed to do. For the most part, these infections run by creating a configuration entry in the **Windows Registry** in order to make these programs start when your computer starts.

Unfortunately, in the Windows operating system, there are many different ways to make a program start which can make it difficult for the average computer user to find manually. Luckily there are programs that allow us to cut through this confusion and see the various programs that are automatically starting when Windows boots. To accomplish this, it is advisable to use an application like a process explorer.

When this type of program is ran, it will list all the various programs that start when your computer is booted into Windows. Most of these programs will be safe, and should be left alone unless know you do not need them to run at startup.

To determine the validity of a process, you can look up the information on the Internet.

Another technique to identifying sources of malware is to examine the most common load points for suspicious entries. This refers to, but is not limited to, analyzing the common load points in the registry.

There are additional items you can look for to find the possible resident malware, this includes thorough examination of your file system to determine out of place or recently added files and checking the Task Manager to determine if any process is using excessive CPU cycles. Boot up analysis can also reveal suspect operations.

Some malware may exist within the execution of your Internet browser by way of Browser Helper Objects(BHO's) and Internet add-ons.

**Process Analysis**

Although the **Task Manager** displays current applications, processes, and services that are running, some malware will conceal itself from being displayed. A more powerful process explorer is recommended. If you are stuck with the **Task Manager** however, be sure to click the button for **Show processes from all users** under the **Process** tab. Examine the processes and services for items that don't

seem to belong, or nonsensical, or randomly generated files names. If you are ever in doubt about what a process or service is, perform an Internet search to determine if it is safe or not.

**Common Load Points:**

This document describes some common loading points for various threats. This document assumes that you have a working knowledge of file management and how to edit the registry.

In Windows 2000 and later operating systems, the most common loading points for these threats are in the registry.

---

**WARNING:** *Symantec strongly recommends that you back up the registry before you make any changes to it. Incorrect changes to the registry can result in permanent data loss or corrupted files. Modify only the keys that are specified.*

---

The loading feature will normally be in the right pane of the following keys and will usually refer to the file name of the threat. Check these keys for suspicious entries:

**HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version\Run**

**HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce**

**HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices**

**HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServicesOnce**

**HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run**

**HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows**

**HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run**

**HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce**

**HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnceEx**

**HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Ru**

**nServices**

**HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServicesOnce**

**HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run**

**HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows**

**HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Win logon**

**HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Windows\AppInit_DLLs**

**HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SharedTaskScheduler**

**HKEY_CLASSES_ROOT\comfile\shell\open\command**

**HKEY_CLASSES_ROOT\piffile\shell\open\command**

**HKEY_CLASSES_ROOT\exefile\shell\open\command**

**HKEY_CLASSES_ROOT\txtfile\shell\open\command**

**HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Win logon**
With this branch selected, look in the right pane for the value: Userinit
This value should contain only C:\WINDOWS\system32\userinit.exe, and have no additional programs specified after the comma.

**HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows**

With this branch selected, look in the right pane for the value: load
This value should be blank.

**Services**
**HKLM\SYSTEM\CurrentControlSet\Services**

**Active Setup Stub Keys (These are disabled if there is a twin in HKCU)**
**HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components**

**ICQ Agent Autostart**
**HKCU\Software\Mirabilis\ICQ\Agent\Apps**

If you suspect that a system is infected, then examine each of these keys. Determine whether Value Name or Value Data, including the (Default) value, refers to a suspicious file.

## THE WININIT.INI FILE

Another file, **C:\Windows\WININIT.INI**, also loads when Windows starts up in normal mode. **WININIT.INI** is used to complete Windows and program installation steps that cannot be completed while Windows is running and, therefore, are deferred until after a reboot. During the boot process, Windows checks to see if there is a WININIT.INI file and, if it finds one, executes its instructions. (After its successful use, it is supposed to be automatically renamed to WININIT.BAK.) You can search for a copy of this file using the Find or Search feature on your Start Menu, and then examine and edit its contents with Notepad. You can temporarily suspend any line of this file by placing a semi-colon in front of the line.

In Windows 2000 and XP, the WININIT.INI file, if exists, will be executed. However it is usually replaced by the "**PendingFileRenameOperations**" sub-key in the Registry key
**HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager.**

### Other load points

Anther possible method that can be used to load an infector is to hide a file and place it (or a shortcut to it) in one of the StartUp folders. In Windows NT-based environments, there can be multiple StartUp folders.

1. On the Windows desktop, right-click **Start** > **Open All Users**.
2. Double-click **Programs**.

3. Double-click **Startup**.
4. Look for any suspicious files. Normally these will be shortcuts, but you may find **.exe, .hta**, or similar files. Be sure to set the view options to Show all files and to display file extensions.
5. Repeat steps 2 through 4 for the current user's StartUp group by right-clicking **Start** and then clicking **Open**.

Less common are loaders that hackers have placed on the system. These can be located in many different locations. In many cases, they can be found only by scanning with your Symantec antivirus product using current definitions.

Due to the nature of the Windows Operating System, many threats run as a process, so that they can be protected by the operating system after they are executed. To look for these, open the Task Manager and look for them on the Processes tab. Because there are many processes running, you must either know the name of a specific process to look up (for example, as described in a virus write-up) or the names of processes that normally run on your computer.

1. Close all programs, saving any work.
2. Press **Ctrl+Shift+Esc** to open the Task Manager.
3. On the Process tab, click **Image Name** twice to sort the processes.
4. Look through the list for possible threats. When a suspicious process is located, select it, and then click **End Process**.
5. You can now locate and delete the loader files, and then remove any load points from the registry.

**<u>Startup Folders:</u>**

**Documents and Settings\All Users\Start Menu\Programs\Startup**
**Documents and Settings\[user name]\Start Menu\Programs\Startup**
**Documents and Settings\Administrator\Start Menu\Programs\Startup**
**Documents and Settings\Default User\Start Menu\Programs\Startup**
**WinNT\Profiles\All Users\Start Menu\Programs\Startup**
**WinNT\Profiles\[user name]\Start Menu\Programs\Startup**
**WinNT\Profiles\Administrator\Start Menu\Programs\Startup**
**WinNT\Profiles\Default User\Start Menu\Programs\Startup**
**Windows\Start Menu\Programs\Startup**
**Windows\All Users\Start Menu\Programs\Startup**

**WinME\Start Menu\Programs\Startup**
**WinME\All Users\Start Menu\Programs\Startup**

**Other Locations:**

**WINDOWS\win.ini**
**Start=**
**Run=**

**WINDOWS\system.ini**
**Shell=**
**Scrnsave.exe=**
**Drivers=**

**Config.sys**
**Autoexec.bat**
**Dosstart.bat**
**Task Scheduler**

## File System

There are many places in the file system that deviant software may decide to call home. The following are a sampling of a few of the most common locations. Open a folder window and switch the viewing mode to sort by date with the current date at the top. Scan the files in the following locations to look for recent modifications or additions:

**%Systemdrive%**
**%Systemdrive%\Windows**
**%Systemdrive%\Windows\System**
**%Systemdrive%\Windows\System32**
**%Systemdrive%\Windows\System32\drivers**

Listed here are some possible TEMP folder locations.

**%systemdrive%\Temp**
**%systemdrive%\Windows\Temp**
**%systemdrive%\Documents and Settings\[User Name]\Local Settings\Temp**
**%systemdrive%\Documents and Settings\Default User\Local Settings\Temp**
**%systemdrive%\Documents and Settings\Administrator\Local**

**Settings\Temp**
**%systemdrive%\Documents and Settings\LocalService\Local Settings\Temp**
**%systemdrive%\Documents and Settings\NetworkService\Local Settings\Temp**

**Windows Update temporary folder:**
**%systemdrive%\WUTemp**
**%systemdrive%\Windows\WUTemp**
**%systemdrive%\Program Files\WindowsUpdate\V4\temp**

## *Network Analysis*

Sometimes the attack can be focused on your networking capability. Hackers can use various tools to open back doors or find open ports already existing on your computer. They can cause your Internet destinations to be redirected to sites of their choosing, use your processing power as part of their botnet, or lock out your Internet connectivity altogether.

### Troubleshooting Network Connectivity

Sometimes, the malware may appear to have disabled your Internet connection. To verify, you will need to do some troubleshooting on your network connectivity.

### Check your Network Status

Open the ***Start Menu*** and go to the ***Control Panel***. Open the ***Network Connections*** icon. Verify the that you are connected to your ***Local Area Connection***, or your ***Wireless Network Connection***. Some computers have multiple connections; ensure that the one you use for Internet connectivity is connected. If all connections show ***Not connected,*** verify your Ethernet cable if connected and your wireless broadband router is powered up and working. In the case of wireless connectivity, you may need to verify your connection setup on both the local computer and the router.

If after checking the above items you still have no connection, you may need to replace your Network Interface Card (i.e. Network or Wireless card).

## Using the Ping Command

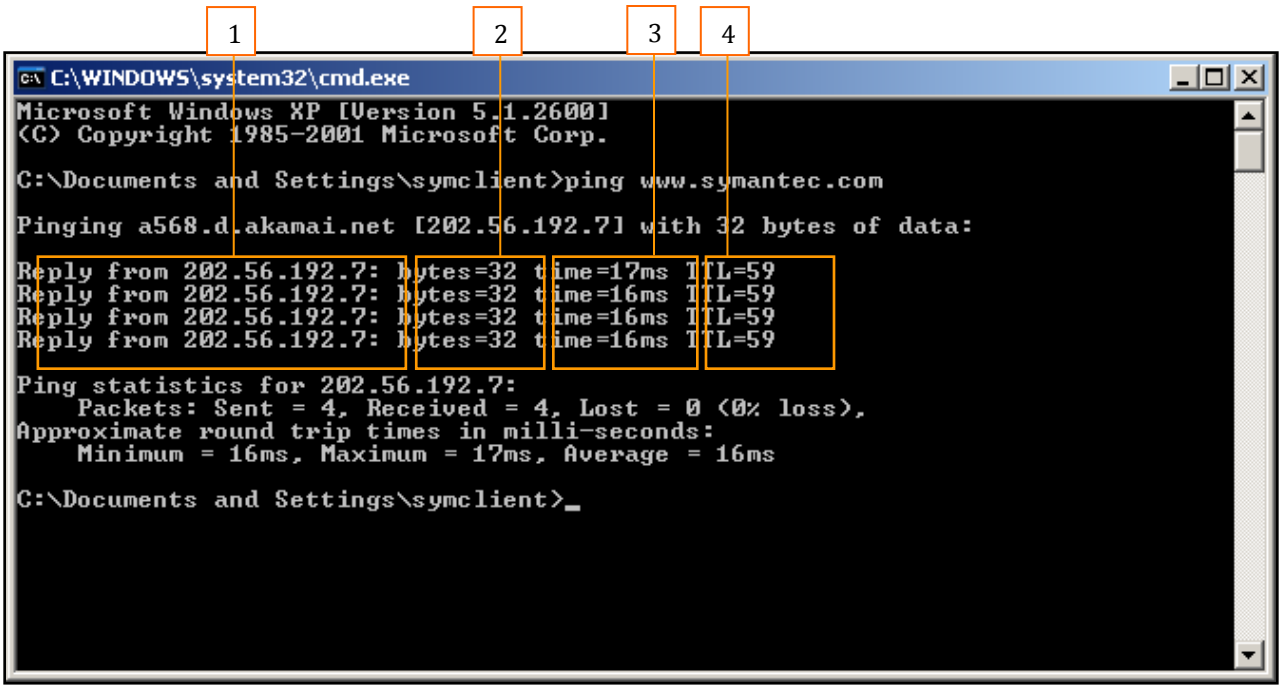
With a viable network connection, you can use the Packet Internet Groper (PING) command to identify the problem with the connectivity between two hosts on a network.

The syntax for the Ping command is:

*Ping* `<IP address> or <hostname>`

Consider a scenario where your machine is infected with a virus. As a first step to rectify this problem, you plan to run an online virus scan. While attempting to reach www.symantec.com, it returns page 404 error. In this case, you can use the Ping command to confirm whether you are connected to the Internet. From the Start Menu, either press the Run button, or click in the search, and type in ***cmd*** to bring up the command line window. Type in "***ping*** www.symantec.com" to ping the Domain Name System address and hit the enter key.

*Your view should be similar to the following:*




1. Indicates that the host was reachable, if the host is not reachable a Request Timeout error message is displayed.

2. Indicates the size of ping packet in bytes.
3. Indicates the response time of ping request.
4. Indicates the time-to-live for ping packet, which is the number of router or hops a pinged packet can traverse before it is discarded.

---

**Tip:** ***To check whether for a problem with the network connectivity or not, ping a machine by the Domain Name System (DNS) name. If it fails, then ping the machine by the IP address. If it succeeds, it indicates a problem with address resolution and not with network connectivity.***

---

**Verify your Internet Protocol address**

From a command prompt type in ***ipconfig /all*** this will display the connection information associated with the network adapters in your computer. An IP address is a label that identifies your computer on the network. It contains 32 bits of information divided into 4 single byte numbers. It can be analogous to a home address with the first section being the country, the second being the city, the third being a street, and the fourth a house number or network node for our purposes. For proper communications and Internet connectivity you will need to makes sure that the IP address and the Default Gateway contain the same first 3 sections of numbers. Your Default Gateway should may have the fourth byte as a 1

Example:

IP address: 192.168.1.101

Default Gateway: 192.168.1.1

**Browser Hijacking and Redirects**

It is not uncommon for malicious software to hijack and redirect your Internet browser. From your ***Control Panel*** open up the ***Internet Options*** icon. Go to the ***Connections*** tab and choose ***Lan Setting.*** In most cases, all boxes should be empty. If you connect through a proxy server please ensure the proper information is in the proxy server box.

**Examine your Hosts file**

Malicious modification of the host file can divert you from arriving at the website you intended to go. In either the Search box, or the Run button from the start menu type in:

%systemroot%\system32\drivers\etc\

To open it, double click on the host file. As no application is associated with this file, you can open it with any text editor. Notepad works well for this function. In the host file you see a lot of information following # signs. Ignore all of that information. Below the # signs should be:

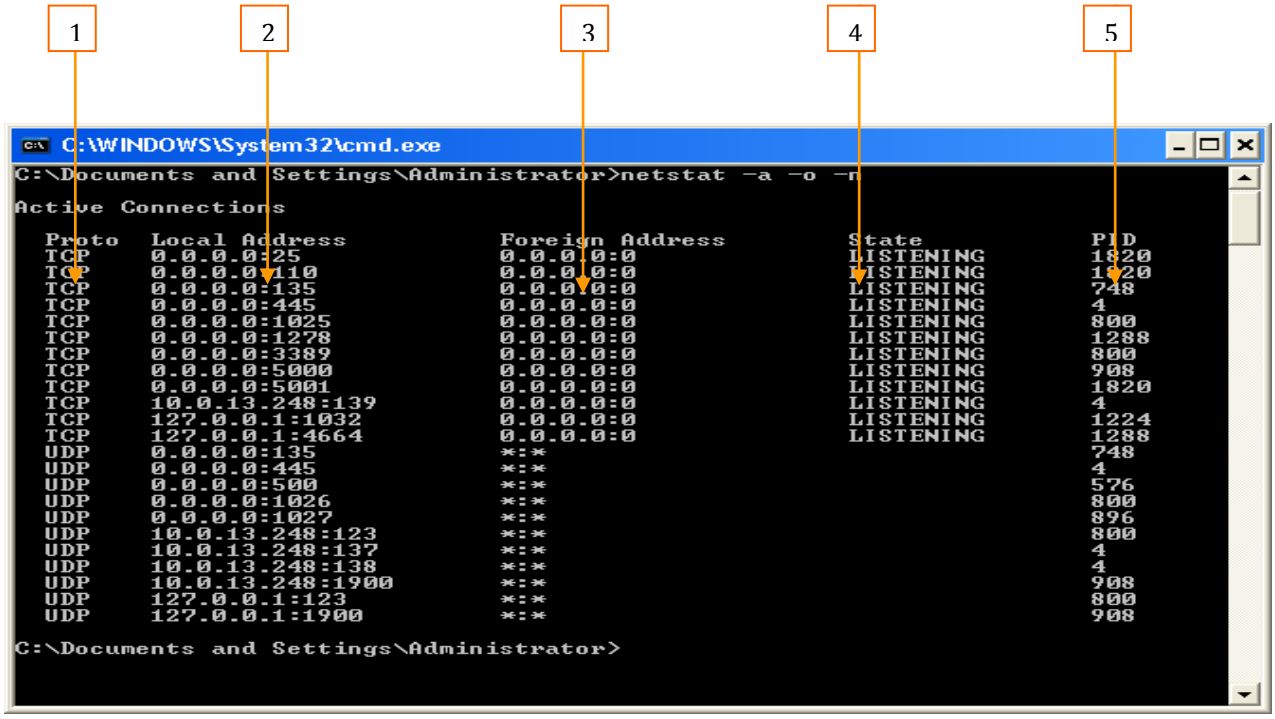
127.0.0.1 localhost

This redirects local traffic back to your computer. A browser redirect can use this area to re-associate DNS addresses to sites of their choosing. If there is any other information aside from that which is listed above, verify its validity before continuing.

## Using the Netstat Command

You can use this command to display all the active TCP/IP connections. By using this command, you can also view the network packet statistics that displays how many packets have been sent and received. The following example demonstrates how to use the Netstat command:

On the command-line, enter **NETSTAT**



**Note:** To view the complete list of the parameters that are associated with the netstat command and its description, type "*netstat /?*" in the command prompt.

1. Indicates the name of the protocol.

2. Indicates the computer name and the port number. When you use the -n parameter with the netstat command, you can view the IP address of the local computer instead of the computer name.

3. Indicates the computer name and the port number of the remote computer. When you use the -n parameter along with the netstat command to view the IP address of the remote computer.

4. Indicates the status of the TCP connection.

5. Indicates the process identifier.

**Tip: Netstat –a –o -n** displays all connections and ports, the process ID of the executables that initiate the connection, the address, and the port numbers.

**Tip: Netstat -a -o -b -n** displays all connections and ports, the executables that create connections, the process ID, the address, and the port numbers.

## Port Types

A computer system utilizes both physical and virtual ports to make connections to the outside world. A physical port can be what the Ethernet cable is plugged into in the back of your computer. A Virtual port is a connection created inside the logic of the computer system that allows for the communication across various channels.

You might be wondering how you can tell valid port usage from a Trojan attack. The good news is that because your regular, normal connections are assigned to low, commonly used ports, in general the higher the number used, the more you should be suspicious. Here are the three main classifications of ports:

**Well Known Ports**

These run from 0 to 1023, and are bound to the common services that run on them. For example, outbound mail runs on channel 25 tcp, which is smtp (Simple Mail Transfer Protocol), so if you find one of these ports open (and you usually will), it's usually because of an essential function. Similarly POP3 connections are often found on Port 110.

**Registered Ports**

These run on 1024 to 49151. Although not bound to a particular service, these are normally used by networking utilities like FTP software, Email client and others. This is done by the opening of a random port within this range before communicating with the remote server. If you do find one of these ports open, it is usually good to be a bit wary as they usually close automatically when the program that's running on them terminates (for example, type in a common website name in your browser with netstat open, and watch as it opens up a port to serve as a buffer.

**Dynamic/Private Ports**

Ranging from 49152 to 65535, these are rarely used except with certain programs, and even then not very often. This is the range most commonly used by Trojan, if any of these ports are open, you should be very suspicious.

For a list of the commonly used Trojan ports see the Appendix .

## *Boot Analysis*

Analyzing your boot-up process can reveal information heretofore yet unrevealed. There are available various utilities for monitoring the boot-up process; for instance, you can use Symantec Systemworks or Microsoft bootVis, or you can enable the Windows default boot up log tool through the Microsoft Configuration Window.

To enter the Microsoft Configuration Window you can either type MSCONFIG into the Search box (Vista, and Windows 7), or click on the run button and enter it in the dialog box (Win2000, XP, etc.).

From the Microsoft Configuration Window choose the Boot Tab (BOOT.INI in Win2000 and XP) and check the boot log box (/BOOTLOG in older versions).

After the next reboot the boot log should be located in C:\Windows\ntbtlog.txt

## *Internet Browser*

### Browser Helper Object (BHO)

Looking for suspicious entries that may have been added as a BHO, is much more complex than looking at the values of the keys as listed previously, as many BHOs are legitimate. In addition, this requires you to look at two different areas in the registry.

1. From the Registry go to:
   **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects**
2. Directly under that key, in the left pane, look for any CLSID sub keys.

   They will look similar to this example:

   {06949E9F-C8D7-4D59-B87D-797B7D6BE0B3}
3. Write down each of the strings that you find (or copy and paste it into Notepad.)
4. Browse to and expand the subkey:
   **HKEY_CLASSES_ROOT\CLSID**<string of letters and numbers>
   where <string of letters and numbers> is what you wrote down in step 3.
5. Under the expanded subkey, select the InProcServer32 key.
6. In the right pane, in the Name and Data columns (including the Default value) look for any file name that may look suspicious, such as random strings of characters or files names that sound out of place.
7. Search either the hard drive or the Web (or both) to either confirm or deny these suspicions. Only if you can confirm that the file name is linked to a malevolent file should you delete the value.

### Add-ons

Add-ons, can also be known as ActiveX controls, browser extensions, browser helper objects, or toolbars, and can be used by a website to provide multimedia or interactive content. Some add-ons can also be used to cause your computer to stop responding or to display undesired content, such as pop-up ads.

If you suspect that browser add-ons are affecting your computer, you might want to disable all add-ons to see if that solves the problem.

To disable all add-ons temporarily

Click the **Start** button, click **All Programs**, click **Accessories**, click **System Tools**, and then click **Internet Explorer (No Add-ons)**.

If disabling all add-ons solves the problem, you might want to use Manage Add-ons to disable all add-ons permanently and then turn on add-ons only as you need them. To disable an add-on, follow the steps below.

To disable add-ons by using Manage Add-ons

Do one of the following:

In Internet Explorer 8, click the **Tools** button, and then click **Manage Add-ons**.

In Internet Explorer 7, click the **Tools** button, point to **Manage Add-ons**, and then click **Enable or Disable Add-ons**.

Do one of the following:

In Internet Explorer 8, under **Show**, click **All Add-ons**.

In Internet Explorer 7, in the **Show** list, click **Add-ons currently loaded in Internet Explorer**.

Click the add-on you want to disable, and then do one of the following:

In Internet Explorer 8, click **Disable**.

In Internet Explorer 7, under **Settings**, click **Disable**.

Repeat the last step for every add-on you want to disable. When you are finished, click **Close** in Internet Explorer 8, or click **OK** in Internet Explorer 7.

## Home Page and Default Search

Your Home Page and Default Search may also be attacked and corrupted. The quickest method to correct your default choices is from within your browser. For **Internet Explorer** can click **Tools** from the toolbar, and from the general tab you can set your home page, or click upon the settings button in the search section to reset your search engine of choice.

## *Safe Mode*

Restarting a PC in safe mode can sometimes bypass the loading of malware into the operating system kernel and allow you additional access for file removal and unblock Internet restrictions. To accomplish this, press F8 before Windows begins to load. You will be presented with a screen with options such as Safe Mode, Safe Mode with Networking, Safe Mode with Command Prompt, etc. At this point, choose the option to start Windows in Safe Mode with Networking. It may take longer than normal for Windows to start, and when it does start, the icons and pictures may appear larger than normal, this is due to the default video drivers having been loaded.

## *Removal*

Now we arrive at the meat of process. In this step you will pit yourself against the deviant programmers, and attempt to reverse their handiwork. It is assumed that you examined the programs running on your computer and found one that does not look right. You did further research by checking that program against a Start Item database or by using an Internet search engine and have learned that it is an infection and you now want to remove it.

If you have identified the particular program or programs that are causing the problems it is often possible to find a well documented solution to its removal. If none are available, the next best course of action is by removing the infected files. Some files may be pivotal to the operation of your operating system, so care must be taken as you move forward.

You will need to remove both the program where it is located on your hard drive as well as the load point previously identified. In many cases the load point will include the path to physical location of the file.

> **It is important to reiterate that malware programs may disguise themselves as valid Microsoft files. It is therefore very important to know exactly which file, and the folder they are in, that you want to remove**.

Once you find the registry entry that is associated with the malware, you will want to delete that entry so it will not start again on the next reboot. Right click on the entry and select **delete**.

Now that we removed it from the sequence, it will not start on boot up, and you can delete the file using My Computer or Windows Explorer.

When you are finished removing the malware entries from the Registry or other load point, and deleted the associated files, reboot into normal mode as your computer should now be clean of the infection.

## *Verification*

After rebooting the computer check for the initial symptoms you observed that made you suspect that you were infected. In addition to this you will want to again check the various load points for any changes or additional suspicious activity.

At this time you may want to run a system scan to verify that the correct Microsoft files are available to the system. To run the System file check you may need your Operating System Disks.

- Open the **Start Menu**
- Click on **Run**
- Type in **CMD** to open a command prompt
- From the command prompt type in:

  **sfc /scannow**

This will take some considerable time to complete.

## *Final Cleanup*

### Clean your Recycle Bin

You may be surprised how many people fail to empty their recycle bin regularly, and it can, if left alone, expand into many megabytes, or even gigabytes! If you have Norton Protected Recycle Bin installed, empty that, too. Right click on the recycle bin and you will see the available options.

### Purge your Temp Folders

Nefarious files, and other general clutter often find refuge in the temp folders. Judicious purging of these folders can free up hard drive space, and prevent unwanted malware reoccurrence.

From the ***Run*** command type in **%temp%**. A Temp window will pop up. Press **Ctrl-A** to select all the files and press delete. If any selected files are currently in use, or otherwise not accessible, unselect that file and continue to delete the files in the folder. Repeat this process in the Windows temp folder (type **temp** from the run box).

## Update your Virus Definitions

Make sure that your Antivirus software shows that it has the latest virus definitions updated.

## Ensure Windows Updates

Some malware disables the ability of your system to perform the necessary Microsoft updates that patch many security issues. Open a browser window and navigate to www.windowsupdate.microsoft.com. Press the Update Windows button and follow the process.

If Windows Updates doesn't function you may need to restart the services associated with it.

- Open the Start Menu
- Click Run or click into the Search box depending on your operating system.
- Type services.msc and then click OK.
- In the list of services look for:
  Windows Update
  Background Intelligent Transfer Service
- Right-click the service name, and then click Properties.
- In the Startup type list, select Automatic.
- Verify that the service status is started.

If the Services cannot be restarted, there may be additional issues.

If all files are correct you may need to register the associated files

- Open the **Start Menu**
- Click on **Run**
- Type in **CMD** to open a command prompt
- In the command prompt type the following commands:
  **Net stop wuaserv**
  **Net stop bits**

For 32-bit Windows, enter the following lines to register the services:

**regsvr32 %windir%\system32\wups2.dll**
**regsvr32 %windir%\system32\oleaut32.dll**
**regsvr32 %windir%\system32\jscript.dll**
**regsvr32 %windir%\system32\vbscript.dll**

**regsvr32 %windir%\system32\msxml.dll**
**regsvr32 %windir%\system32\softpub.dll**
**regsvr32 %windir%\system32\wintrust.dll**
**regsvr32 %windir%\system32\initpki.dll**
**regsvr32 %windir%\system32\cryptdlg.dll**

For 64-bit Windows, the path differs due to the location of the DLL file:

**regsvr32 %windir%\syswow64\wups2.dll**
**regsvr32 %windir%\syswow64\oleaut32.dll**
**regsvr32 %windir%\syswow64\jscript.dll**
**regsvr32 %windir%\syswow64\vbscript.dll**
**regsvr32 %windir%\syswow64\msxml.dll**
**regsvr32 %windir%\syswow64\softpub.dll**
**regsvr32 %windir%\syswow64\wintrust.dll**
**regsvr32 %windir%\syswow64\initpki.dll**
**regsvr32 %windir%\syswow64\cryptdlg.dll**

For both versions

**Net Start wuaclt**
**Net Start bits**

You may need to reset your computer at this time.

If you wish to enable automatic updates follow the steps below.
Make sure Windows Update is active by typing in **Security Center** into the **Search** box for **Vista** or **Windows 7**, and opening up the security portion. Check to ensure that Updates are enabled.

If using **XP** or earlier, from the **Run** dialog box type **sysdm.cpl**. This will bring up the **System Properties** window. Choose the **Automatic Updates** tab and choose **Automatic (recommended)**, and press **OK**.

## Reset System Restore

By turning System Restore off and then back on again, you can purge the system of possibly corrupted Restore Points.

**Steps to turn off System Restore**

- Open the **Start** menu

- Right-click **My Computer**
- Click **Properties**.
- In the **System Properties** dialog box (for Vista & Win7 click on **System Protection**, click the **System Restore** tab.
- Click to select the **Turn off System Restore** check box. Or, click to select the **Turn off System Restore on all drives** check box.
- Click **Apply**.
- When you receive the following message, click **Yes** to confirm that you want to turn off System Restore:

  You have chosen to turn off System Restore. If you continue, all existing restore points will be deleted, and you will not be able to track or undo changes to your computer.

  Do you want to turn off System Restore?

**Steps to turn on System Restore**

- Click to clear the **Turn off System Restore** check box. Or, click the **Turn off System Restore on all drives** check box.
- Click **OK**.

**<u>Set Restore Point</u>**

**Windows XP**

To set a System Restore Point...

- Open the **Start menu**
- Open the **Programs menu**
- Open the **Accessories menu**
- Open the **System Tools menu**
- Start **System Restore**

- Pick the option for setting a System Restore Point and click on the **Next** button
- Fill in a name for the restore point so you can find it and click on the **Create** button
- Click on the **Close** button when done

**Windows Vista & Windows 7**

- Open **Start** menu
- Click on the **search** box
- Type **Create Restore Point**.
- Choose the drive you want the restore point to be on.
- Press the **Create** button
- Name the Restore point
- Press the **Create** button

## Reset File Views

File views should be reset so as not to interfere with day to day operations. In XP and older operating systems, to access the folder options settings, you can open **Folder Options** in the **Control Panel**, or from a folder window by clicking **Tools**, and then **Folder Options**. In Vista and Windows 7 you can type **Folder Options** into the **Search Bar**.

Once you open the **Folder Options** window select the **Advanced tab**, and under **Hidden Files and Folders** unselect **show hidden files, folders, and drives**. In addition to this check the boxes next to **Hide extensions for known files types**, and **hide protected operating system files**.

## Restore UAC (Microsoft Vista & Windows 7)

From the **Search Box** type in **UAC** from here you have the option to turn User Access Control back on.

## *Virus Removal Examples*

**Infostealer.Banker.C**

Check this link for more information on **Backdoor.Paproxy (Symantec)** and also known as **Infostealer.Banker.C**

**File information (included for familiarization of identification process)**

MD5: da4b7ef93c588ad799f1a1c5afb6cfad
SHA1: 4d6ba16306ea54da47b9e1381d8c5ed27313e414
SHA256: 9703eecd3ba1fe50ed88293c4e8fbaed1601d7adb2d2bf691266f5842a02d28e
SHA512:bdb313698dc14e78ce40bed3fa678842f5ebfe99e5615f76e524ebb8b7fe2e79278a8a9bf1339c7ea19b1abec9d95643600697dfd3649d40fd6fbcf52393533c

Delete the below mentioned files.

**Physical Location**

C:\WINDOWS\SYSTEM32\IHP3K7~1.HTM

C:\Documents and Settings\All Users\Documents\Settings\winsys2f.dll

C:\WINDOWS\system32\ntos.exe
C:\WINDOWS\system32\wsnpoem\audio.dll
C:\WINDOWS\system32\wsnpoem\video.dll
C:\WINDOWS\system32\wudb.dll
C:\WINDOWS\wr.txt
C:\WINDOWS\Temp\win*.tmp

**Registry Location**

HKLM\SOFT\MS\WINNT\WINLOGON\ -
UserInit=D:\WINDOWS\system32\Userinit.exe,C:\WINDOWS\system32\ntos.exe

Delete this entry.

**KB Recommended: Backdoor.Paproxy (Symantec AV / N360)**

The email itself remains the same but the attachment name contains now a tracking number like **UPS_INVOICE_978172.exe.**

The .exe is a new variant and when submitting an example to Virus Total only **3 of the 34 antivirus engines detected this new variant**. More details below in the table.

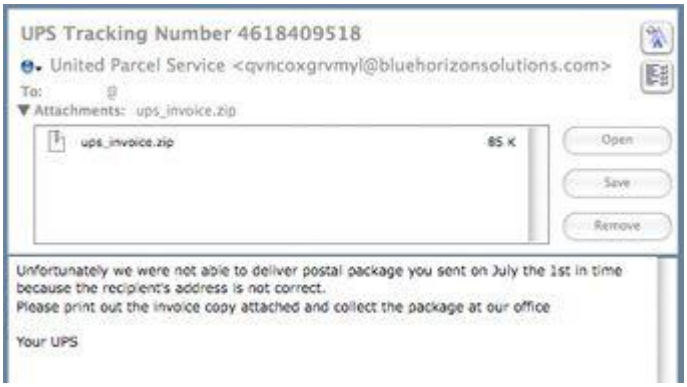
**eSafe7.0.17.02008.07.21Suspicious File**

**F-Secure7.60.13501.02008.07.21Suspicious:W32/Malware!Gemini**

**Symantec102008.07.21-**

**VBA323.12.8.12008.07.21suspected of Malware-Cryptor.Win32.General.2**

Find the screen shot of its attached email




The file contains threat characteristics of ZBot - a banking Trojan that disables firewall, steals sensitive financial data (credit card numbers, online banking login details), makes screen snapshots, downloads additional components, and provides a hacker with the remote access to the compromised system. It opens backdoors on infected computer to allow malicious attacker unauthorized access.

On an infected computer the trojan will create a new files like **%System%\ntos.exe, %System%\wsnpoem\audio.dll, %System%\wsnpoem\video.dll and creates a new directory %System%\wsnpoem.**

It also adds and modifies entries in the Windows registry and make connection with a server for http://*********.ru/******/odessa.bin. It opens random TCP ports in order to provide backdoor capabilities.

Removal instruction as of now

- Remove the entries relevant to the above file names
- Empty the Recycle bin
- Reset the IE web settings
- Delete the Temp/Prefetch

**Trojan.DNSChanger-Symantec**

**Trojan.Flush.K** also known as **Trojan.DNSChanger-Symantec** is a trojan that makes Internet Explorer open slowly and redirects valid links to malicious or advertisement links. The issue occurrences have been identified by knowing from a customer. He had tried to download some videos from LIMEWIRE and ended to COX-DNS issue. The .Dll files creates its own Process in following areas of (Library, Module and Services-Svchost.exe)

Files involved in this infection:
C:\Windows\System32\msliksurdns.dll
C:\Windows\System32\msliksurcredo.dll
C:\Windows\System32\Drivers\msliksurserv.sys

\??\globalroot\systemroot\system32\drivers\msliksurserv.sys

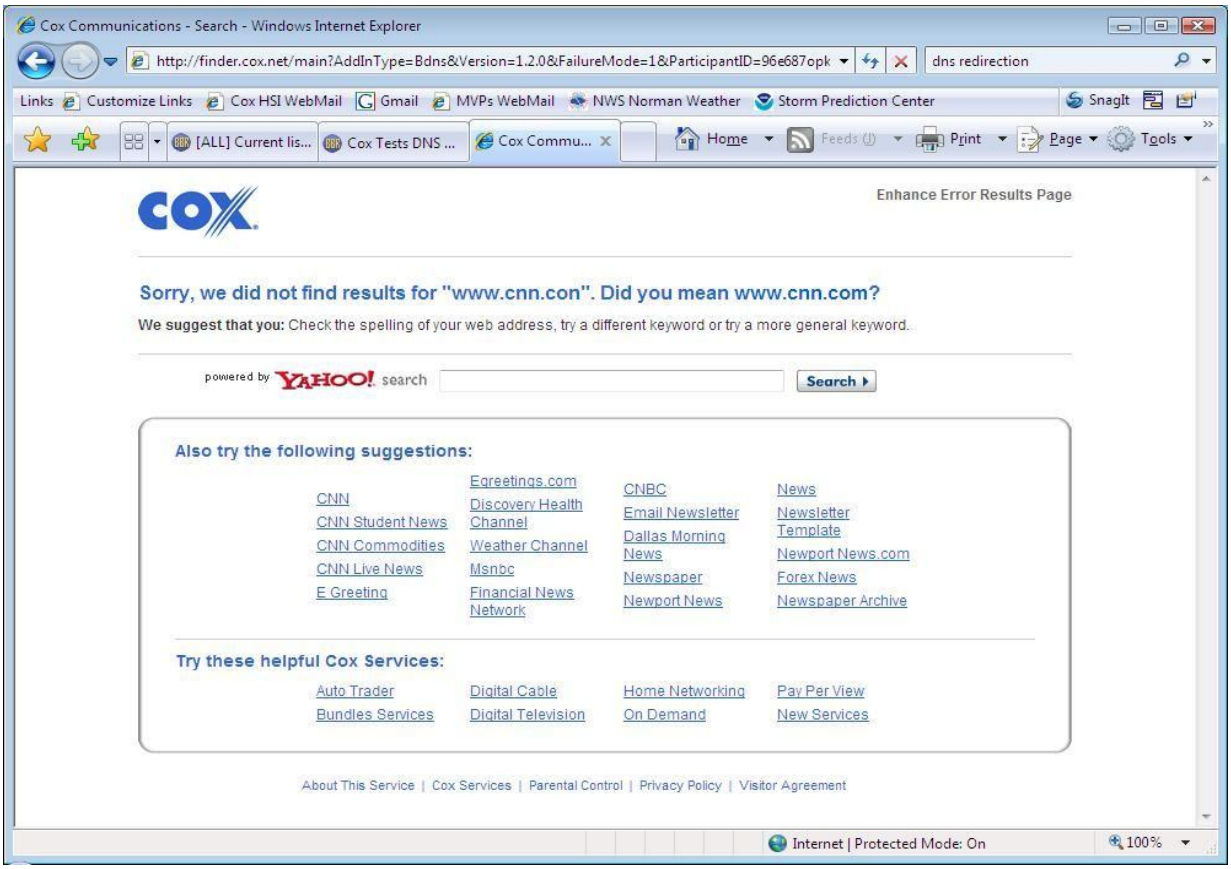
**File Information: (included for indentification only)**

**msliksurserv.sys** received on 07.13.2008 15:31:55 (CET)
File size: 14848 bytes
MD5...: 9888deaaea64d355db5394c15322ce09

**msliksurcredo.dll** received on 07.13.2008 16:12:37 (CET)
File size: 65536 bytes
MD5...: f6fb1ed12ff60a7854c83f97a26de927
**msliksurdns.dll** received on 07.13.2008 16:12:44 (CET)
File size: 21504 bytes
MD5...: e966f3be5fce6f4c09efb84263082542

**Symptoms**

When a user types the URL in the address bar, the website is redirected to the COX.net warning page stating the computer is infected. Sometimes they also appear like the screenshot displayed when a page is mis-typed.




## Solution

**For WINDOWS XP**

For Users on a Dial-up Connection:

Go to My Computer>**Dialup Networking**.

Right-click your internet connection and select **Properties**.

A window will open - click the **Server Types** tab. Click **TCP/IP Settings**.

For All Other Users:

Go to Control Panel>**Network Connections** and select your local network.

Click **Properties**, then select **Internet Protocol (TCP/IP).**

Click **Properties.**

You may find any of these listed DNS Add under option "*Use the Following DNS Addresses*" *( Preferred & Alternate).*

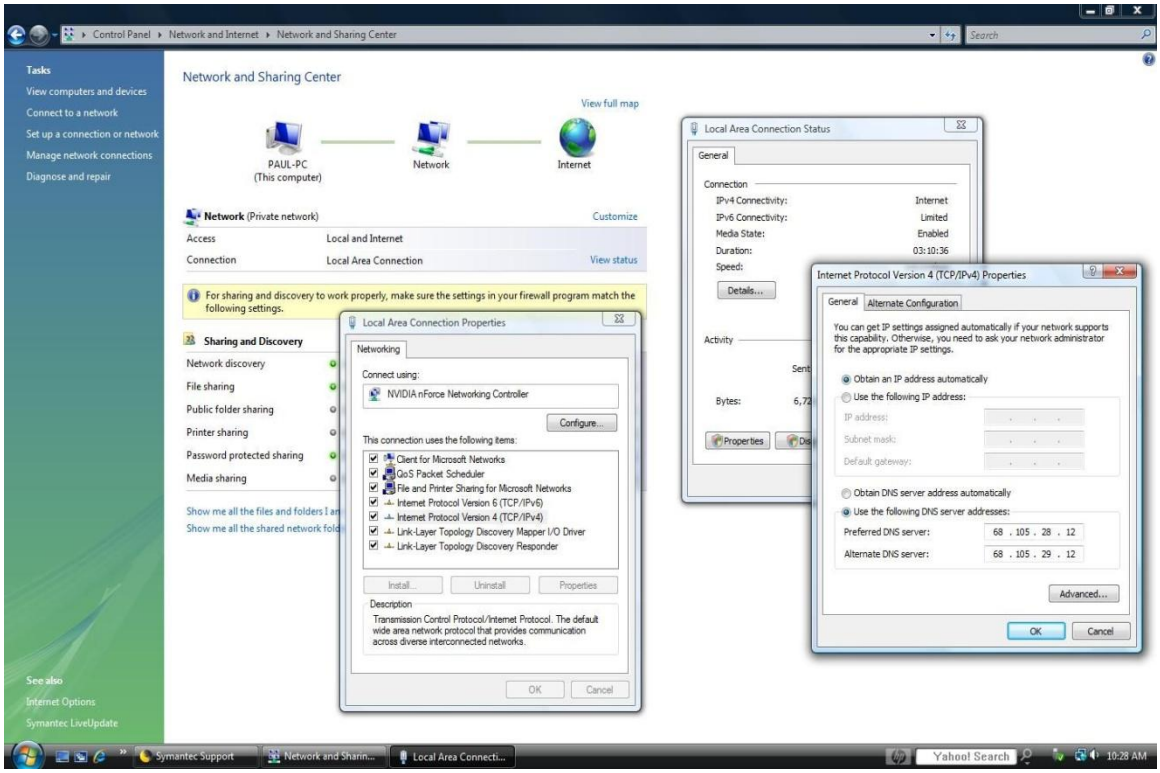
Change it to the other option "**Obtain DNS server address automatically**"

**68.105.28.11**

**68.105.29.11**
**68.105.28.12**

**For WINDOWS Vista**

Find the screen shot which depicts the location (Go to Control Panel>Network and Sharing Center>Local Area Connection>View Status>TCP/IP v4>Properties>General>Change it to the other option "**Obtain DNS server address automatically**"




- Then search and delete the following files by making them unhidden with the Folder Option for View File types.

C:\Windows\System32\msliksurdns.dll
C:\Windows\System32\msliksurcredo.dll
C:\Windows\System32\Drivers\msliksurserv.sys

- Reset the IE web settings
- Delete all temp/prefetch/%temp% and empty the recycle bin
- Reboot and Reconnect back in the normal mode
- Run the LU and Full system scan along with MS Windows Update.

# *OS Considerations*

## *XP*

XP is the most common platform targeted by today's malware. If you are using XP make sure that it's updated with the latest service patch. Antivirus and security software is a must. A fresh install of XP connected to the Internet can become infected with some form of malware if not protected within minutes.

## *Vista*

Improved security was a primary design goal for Vista. Microsoft's Trustworthy Computing initiative, which aims to improve public trust in its products, has had a direct effect on its development. This effort has resulted in a number of new security and safety features.

The addition of the User Account Control, or UAC is perhaps the most significant and visible of these changes. UAC is a security technology that makes it possible for users to use their computer with tighter privileges by default, with the goal of stopping malware from making unauthorized changes to the system.

Testing by Symantec Corporation has proved the effectiveness of UAC. Symantec used over 2,000 active malware samples, consisting of backdoors, Keyloggers, Rootkits, Mass mailers, Trojan horses, Spyware, Adware, and various other samples. Each was executed on a default Windows Vista installation within a standard user account. UAC effectively blocked over 50 percent of each threat, excluding rootkits. Five percent or less of the malware which evaded UAC survived a reboot.

As part of the redesign of the network stack, Windows Firewall has been upgraded, with new support for filtering both incoming and outgoing traffic. Advanced packet filter rules can be created which can grant or deny communications to specific services.

The 64-bit versions of Vista require that all device drivers be digitally signed, so that the creator of the driver can be identified.

## *Win7*

While no operating system is perfect, Microsoft appears to have made significant security improvements with the release of Windows 7.

**Action Center**. The Action Center is responsible for **overall maintenance and security on Windows 7**. The Security Center that was on Vista has been absorbed into the Action Center. Users are notified of changes in the system on the taskbar.

**Changes to User Account Control**. User Account Control (UAC) was one of the most maligned aspects of Vista, as it repeatedly asked user permission for administrative applications. You could turn off the function, but would run the risk of downloading unwanted software. Windows 7 gives the user more options on how and when it provides notifications.

## *64-bit Operating Systems*

One reason Windows and applications such as Internet Explorer are the target of more attacks is because for the attacker, they present a much larger attack surface than operating systems and applications that have a much lower market share. Although "security through obscurity" is held in disdain by most security pundits, it does work to the extent that more obscure targets attract fewer attacks. As 64 bit operating systems have less market presence, not as much malware has been written for them. This will change as they become more widely integrated and 32 bit systems are phased out.

In 2004, Symantec reported the first virus written to infect 64 bit machines, called Shruggle. In May 2005 they reported a second 64 bit virus, written to infect Windows portable executables (PE files), called Rugrat. These won't run on 32 bit platforms and were apparently created as proof of concept viruses, with very few infections ever reported.

This is not to say that a 64 bit system is protected from all malware written for 32 bit computers. Most 32 bit programs will run in a 32 bit mode on a 64 bit OS. The programs

will not have access to the kernel mode though. This provides some resistance against many of the most dangerous malicious programs.

There are more good news: the current rootkits that have been written for 32 bit systems, including the infamous Sony music CD rootkit, don't work in the 64 bit OS. When updating the kernel code for the 64 bit version, Microsoft programmers took the opportunity to include code that is part of the kernel that makes it impossible to install a patch in a running kernel (which kernel mode rootkits do on 32 bit systems).

Likewise, processor vendors had an opportunity, in making the new 64 bit processors, to include security mechanisms. Both AMD and Intel include code in their 64 bit products to prevent the exploitation of buffer overflow and buffer under-run conditions.

# *Professional Assistance*

If you need professional assistance to detect and remediate your infected computer, please visit http://www.symantec.com/norton/support/premium_services/premium_virus.jsp to take advantage of our Spyware and Virus Removal service.

# *Additional Information*

## *Introduction to Safe Computing*

Home computers are a popular target for intruders. This is due to the fact that home computers usually use less complex protection and take less work and risk to penetrate than the systems within a secure enterprise network. This is not to say that in the past, hackers haven't also provided equal headaches for the security administrators in big enterprises, exploiting every possible opportunity to sneak in. The attackers look for credit card numbers, bank account information, and anything else they can find from your home computer. But it's not just the money-related information they're after. Intruders also want the compromised computer's resources, to attack other computers on the Internet. In fact, the more computers an intruder uses, the harder it is for law enforcement to figure out where the attack is really coming from.

Not many of the home computer users are aware of the security issues that can arise out of unsafe computing practices, unless they experience an attack on their computers. When combined with high-speed Internet connections that are always turned on, intruders can quickly find and then attack home computers. While intruders also attack home computers connected to the Internet through dial-up connections, high-speed connections (cable

modems and DSL modems) becomes a favored target. As we have discussed earlier, attackers use various methods such as attaching a virus in an email, to enter or access the home computers. They also take advantage of a vulnerabilities in the computer's programs code to gain access.

What follows are some tips to help provide a more secure computing experience.

**Install and Use an Anti-Virus Program**

An anti-virus program is value-add to a home computer. Though, a newly purchased computer might include a trial version that the PC manufacturer provides with. Operating system manufacturers usually provide a recommendation to the users to buy security software to ensure a safe computing experience. However, as we have discussed earlier, as the threat behavior keeps changing, the anti-virus program should also keep itself current to keep the computer protected from the attacks. Hence, the customers need to constantly update the software with the latest definitions and signatures. Intruders are the most successful in attacking all computers – not just home computers – when they use viruses and worms. Installing an anti-virus program and keeping it up to date is among the best defenses for a home computer.

**Patch the Operating System**

Similar to the way fabric patches are used to repair holes in clothing, software patches repair holes in software programs. Patches are updates that fix a particular problem or vulnerability within a program. Sometimes, instead of just releasing a patch, vendors will release an upgraded version of their software, although they may refer to the upgrade as a patch. Software vendors usually provide patches to their software that are supposed to fix the bugs in it.

Operating system manufacturers also provide patches to fix the vulnerabilities in it. Windows provides security updates to fix the vulnerabilities and keep the operating system protected against any threats. These updates are available on the Web for you to download and install on the system. However, Windows operating system has the automatic update feature that downloads the security updates whenever they are available in the Windows website. This feature when turned on, checks periodically for the Windows Update website for high-priority updates that can help protect the computer against attacks. High-priority updates include security updates, critical updates, and service packs. This is a key feature that keeps

operating system protected while it downloads the latest security updates without the user initiation.

The scheduled updates provide the following benefits:

- **Convenience**: Automatic updates looks for security updates, critical updates, and service packs, and installs them on the schedule that is set.
- **Reliability**: Updates are downloaded behind the scenes whenever the users are connected to the Internet. The downloading process doesn't interfere with other downloads or interrupt the work. If disconnect from the Internet before updates are fully downloaded, the download process will continue the next time the computer is connected to the Internet.
- **Up-to-date software**: Users can set the schedule for Windows to install new updates. This means that Windows is checking periodically for and installing any important updates that the computer needs.

For instructions on how to turn on automatic updates see here.

**Handle Emails with Care**

Email attachments need to be scanned before opening. This helps the Anti-virus programs to trap and identify the malware in the attachment. It is always a safe practice to avoid reading attachments from an unknown email address. Especially, malicious attachments are usually enticing to open. It is safe to scan the attachment for malware before opening them.

**Social Engineering Attacks:**

Social engineering is a collection of techniques used to manipulate people into performing actions or divulging confidential information. To launch a social engineering attack, an attacker uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems. An attacker may seem unassuming and respectable, possibly claiming to be a new employee, repair person, or researcher and even offering credentials to support that identity.

However, by asking questions, he or she may be able to piece together enough information to infiltrate a network. If an attacker is not able to gather enough information from one source, he or she may contact another source within the same organization and rely on the information from the first source to add to his or her credibility.

With attackers focusing on socially engineered attacks, there is a high likelihood that the email containing a malicious attachment might even come from someone posing as a reliable source. It makes for a good safety guideline to always have an anti-virus program scan the emails and attachments before opening it, irrespective of whether it comes from a known or unknown source.

## Install a Firewall

Firewalls provide protection against outside attackers by shielding your computer or network from malicious or unnecessary Internet traffic. Firewalls can be configured to block data from certain locations while allowing the relevant and necessary data through. They are especially important for users who rely on "always on" connections such as cable or DSL modems.

Firewalls are offered in two forms: hardware (external) and software (internal). While both have their advantages and disadvantages, the decision to use a firewall is far more important than deciding which type to use. There are two types of firewalls that you can use. They are:

- Hardware - Typically called network firewalls, these external devices are positioned between your computer or network and your cable or DSL modem. Many vendors and some Internet Service Providers (ISPs) offer devices called "routers" that also include firewall features. Hardware based firewalls are particularly useful for protecting multiple computers but also offer a high degree of protection for a single computer. If you only have one computer behind the firewall, or if you are certain that all of the other computers on the network are up to date on patches are free from viruses, worms, or other malicious code, you may not need the extra protection of a software firewall. Hardware based firewalls have the advantage of being separate devices running their own operating systems, so they provide an additional line of defense against attacks.

- Software – Norton Antivirus products as well as some operating systems include a built-in firewall; if yours does, consider keeping it enabled to add another layer of protection even if you have an external firewall. Because of the risks associated with downloading software from the Internet onto an unprotected computer, it is best to install the firewall from a CD, DVD, or floppy disk. Although relying on a software firewall alone does provide some protection, realize that having the firewall on the same computer as the information you're trying to protect

may hinder the firewall's ability to catch malicious traffic before it enters your system.

Most commercially available firewall products, both hardware or software based, come configured in a manner that is acceptably secure for most users. Since each firewall is different, you'll need to read and understand the documentation that comes with it in order to determine if the default settings on your firewall are sufficient for your needs. Additional assistance may be available from your firewall vendor or your ISP (either from tech support or a web site).

**Backup files periodically**

Backing up your files periodically protects your system from possible data loss. It is always a safe computing practice to run a backup of some important files and folders in your computer.

Consider taking a backup on the following parameters:

- Files: What files should you back up? The files you select are those that you can neither easily recreate nor reinstall, such as the CD-ROMs or the floppy disks that came with your computer.

- Frequency: How often should you back them up? In the best of all cases, you should back up a file every time it changes. If you don't, you'll have to reintroduce all the changes that happened since your last backup.

- Media: Where should you back them up to; that is, what media should you use to hold backed up files? The answer is: whatever you have. It's a question of how many of that media you have to use and how convenient it is. For example, most computers have a floppy disk drive. You could back up your irreplaceable files to floppies. That process just takes lots of time and may not be as convenient as using another media. Larger capacity removable disk drives and writable CD-ROMs also work well, take less time, and are more convenient.

If you don't have a backup device, there are alternatives. There are Internet services that let you back up your files to a centralized location. Some of these services provide "transparent access" to the backups. That is, they look like another hard drive attached to your computer. You use the file copy scheme that your computer

provides to back up files and recover them from backed up storage. One such service is Norton Online Backup.

## Use (strong) Passwords

Passwords are a common form of authentication and are often the only barrier between a user and your personal information. There are several programs attackers that can use to help guess or "crack" passwords, but by choosing good passwords and keeping them confidential, you can make it more difficult for an unauthorized person to access your information.

**Why do you need a password**?

Think about the number of PIN numbers or passwords that you use every day: getting money from the ATM or using your debit card in a store, logging on to your computer or email. Keeping track of all of the number, letter, and word combinations may be frustrating at times, and maybe you've wondered if all of the fuss is worth it. After all, what attacker cares about your personal email account, right? Or why would someone bother with your practically empty bank account when there are others with much more money? Often, an attack is not specifically about your account. While having someone gain access to your personal email might not seem like much more than an inconvenience and threat to your privacy, it is about using the access to your information to launch a larger attack.

Passwords are the most common means of authentication, but if you don't choose good passwords or keep them confidential, they are almost as ineffective as not having any password at all. Many systems and services have been successfully broken into due to the use of insecure and inadequate passwords, and some viruses and worms have exploited systems by guessing weak passwords.

**How do you choose a good password?**

Most people use passwords that are based on personal information and are easy to remember. However, that also makes it easier for an attacker to guess or "crack" them. Consider a four-digit PIN number. Is yours a combination of the month, day, or year of your birthday? Is it the last four digits of your social security number? Is it your address or phone number? Think about how easily it is to find this information out about somebody. What about your email password, is it a word that

can be found in the dictionary? If so, it may be susceptible to "dictionary" attacks, which attempt to guess passwords based on words in the dictionary.

Although intentionally misspelling a word ("daytt" instead of "date") may offer some protection against dictionary attacks, an even better method is to rely on a series of words and use memory techniques, or mnemonics, to help you remember how to decode it. For example, instead of the password "hoops," use "IlTpbb" for "[I] [l]ike [T]o [p]lay [b]asket[b]all." Using both lowercase and capital letters adds another layer of obscurity. Your best defense, though, is to use a combination of numbers, special characters, and both lowercase and capital letters. Change the same example we used above to "Il!2pBb." and see how much more complicated it has become just by adding numbers and special characters.

Don't assume that now that you've developed a strong password you should use it for every system or program you log into. If an attacker does guess it, he would have access to all of your accounts. You should use these techniques to develop unique passwords for each of your accounts.

Here is a review of tactics to use when choosing a password:

- Don't use passwords that are based on personal information that can be easily accessed or guessed
- Don't use words that can be found in any dictionary of any language
- Develop a mnemonic for remembering complex passwords
- Use both lowercase and capital letters
- Use a combination of letters, numbers, and special characters
- Use different passwords on different systems

**How can you protect your password?**

Now that you've chosen a password that's difficult to guess, you have to make sure not to leave it someplace for people to find. Writing it down and leaving it in your desk, next to your computer, or, worse, taped to your computer, is just making it easy for someone who has physical access to your office. Don't tell anyone your passwords, and watch for attackers trying to trick you through phone calls or email messages requesting that you reveal your passwords.

There are some simple habits that you can adopt. These habits when followed consistently reduce the chances that the information on your computer will be lost or corrupted.

**How can you minimize the access other people have to your information?**

You may be able to easily identify people who could, legitimately or not, gain *physical* access to your computer—family members, roommates, co-workers, members of a cleaning crew, and maybe others. Identifying the people who could gain *remote* access to your computer becomes much more difficult. As long as you have a computer and connect it to a network, you are vulnerable to someone or something else accessing or corrupting your information; however, you can develop habits that make it more difficult.

- **Lock your computer when you are away from it:** Even if you only step away from your computer for a few minutes, it's enough time for someone else to destroy or corrupt your information. Locking your computer prevents another person from being able to simply sit down at your computer and access all of your information.
- **Disconnect your computer from the Internet when you aren't using it:** The development of technologies such as DSL and cable modems have made it possible for users to be online all the time, but this convenience comes with risks. The likelihood that attackers or viruses scanning the network for available computers will target your computer becomes much higher if your computer is always connected. Depending on what method you use to connect to the Internet, disconnecting may mean ending a dial-up connection, turning off your computer or modem, or disconnecting cables.
- **Evaluate your security settings:** Most software, including browsers and email programs, offers a variety of features that you can tailor to meet your needs and requirements. Enabling certain features to increase convenience or functionality may leave you more vulnerable to being attacked. It is important to examine the settings, particularly the security settings, and select options that meet your needs without putting you at increased risk. If you install a patch or a new version of the software, or if you hear of something that might affect your settings, reevaluate your settings to make sure they are still appropriate.

# *Appendix*

## *Ports Commonly Used by Trojans*

Please note that this isn't a complete list, but it will provide an idea of what to look out for in Netstat. Be aware that some of the lower Ports may well be running valid services.

| Port # | Protocol | General Description |
|---|---|---|
| 1 | TCP | Socks Des Troie |
| 2 | TCP | Death |
| 8 | ICMP | Ping Attack |
| 20 | TCP | Senna Spy |
| 21 | TCP | FTP service, Dolly Trojan |
| 22 | TCP | Shaft |
| 23 | TCP | Fire Hacker |
| 25 | TCP | Trojans & Worms using this port |
| 31 | TCP | Agent 31, Hacker's Paradise |
| 37 | TCP | Trojans & Worms using this port |
| 41 | TCP | Deep Throat |
| 53 | TCP | Trojans & Worms using this port |
| 58 | TCP | DM Setup |
| 69 | TCP | Trojans & Worms using this port |
| 70 | TCP | W32.Evala.Worm |
| 79 | TCP | Firehotcker |
| 80 | TCP | Trojans & Worms using this port |
| 81 | TCP | Beagle.S |
| 85 | TCP | Common Port for phishing scam sites |
| 87 | TCP | Common Port for phishing scam sites |
| 88 | TCP | pwsteal.likmet.a |
| 90 | TCP | Hidden Port 2.o |
| 99 | TCP | Common Port for phishing scam sites |
| 110 | TCP | ProMail Trojan |
| 113 | TCP | Trojans & Worms using this port |
| 119 | TCP | Happy99 |
| 121 | TCP | Jammer Killah |
| 129 | TCP | Password Generator Protocol |
| 135 | TCP UDP | Trojans & Worms using this port |

| | | |
|---|---|---|
| 137 | TCP UDP | Netbios name (DoS attacks) |
| 138 | TCP UDP | Netbios datagram |
| 139 | TCP UDP | Netbios session (DoS attacks) |
| 146 | TCP | Infector 1.3 |
| 382 | TCP | W32.Rotor |
| 420 | TCP | W32.kibuv.b |
| 421 | TCP | Tcp Wrappers |
| 443 | TCP | Trojans & Worms using this port |
| 445 | TCP | Trojans & Worms using this port |
| 456 | TCP | Hacker's Paradise |
| 530 | TCP | W32.kibuv.worm |
| 531 | TCP | Rasmin |
| 555 | TCP | Stealth Spy, Phaze, 7-11 Trojan |
| 559 | TCP | Trojans & Worms using this port |
| 587 | TCP | Sober worm Variants |
| 666 | TCP | Attack FTP |
| 666 | UDP | N0kN0k Trojan |
| 777 | TCP | BackDoor.Netcrack.B |
| 778 | TCP | BackDoor.Netcrack.B |
| 880 | TCP | Common Port for phishing scam sites |
| 901 | TCP | Backdoor.Devil |
| 902 | TCP | Backdoor.Devil |
| 911 | TCP | Dark Shadow |
| 999 | TCP | DeepThroat |
| 1000 | TCP | Der Spaeher |
| 1001 | TCP | Backdoor.Wortbot |
| 1011 | TCP | Doly Trojan |
| 1012 | TCP | Doly Trojan |
| 1015 | TCP | Doly Trojan |
| 1024 | TCP | Backdoor.lingosky |
| 1025 | TCP | Trojans & Worms using this port |
| 1025 | UDP | Maverick's Matrix 1.2 - 2.0 |
| 1033 | TCP | NetSpy |
| 1034 | TCP | Trojans & Worms using this port |
| 1042 | TCP | Bla |
| 1045 | TCP | Rasmin |
| 1080 | TCP | Trojans & Worms using this port |

| | | |
|---|---|---|
| 1081 | TCP | Backdoor.Zagaban |
| 1111 | TCP | Trojans & Worms using this port |
| 1218 | TCP | Backdoor.Sazo |
| 1234 | TCP | Trojans & Worms using this port |
| 1243 | TCP | Sub Seven |
| 1245 | TCP | VooDoo Doll |
| 12345 | TCP | Backdoor.Amitis.B |
| 1269 | TCP | Maverick's Matrix |
| 12631 | TCP | WhackJob |
| 1349 | UDP | BackOrifice DLL Comm |
| 1394 | TCP | GoFriller, Backdoor G-1 |
| 1433 | TCP | w32.spybot.ofn |
| 1492 | TCP | FTP99CMP |
| 1505 | TCP UDP | FunkProxy |
| 1509 | TCP | Psyber Streaming server |
| 1533 | TCP | Backdoor.Miffice |
| 1534 | TCP | Bizex.Worm |
| 1600 | TCP | Shivka-Burka |
| 1604 | TCP UDP | ICA Browser |
| 1751 | TCP | Loxbot.d |
| 1772 | TCP | Backdoor.NetControle |
| 1807 | TCP | SpySender |
| 1863 | TCP | Trojans & Worms using this port |
| 1981 | TCP | Shockrave |
| 1999 | TCP | BackDoor.BiFrose |
| 2000 | TCP UDP | BackDoor.Fearic |
| 2001 | TCP | Trojan Cow |
| 2002 | TCP | TransScout |
| 2003 | TCP | TransScout |
| 2004 | TCP | TransScout |
| 2005 | TCP | TransScout |
| 2023 | TCP | Ripper |
| 2041 | TCP | W32.korgo.a |
| 2080 | TCP | Backdoor.TJServ |
| 2090 | TCP | Backdoor.Expjan |
| 2115 | TCP | Bugs |
| 2140 | TCP | Deep Throat |

| | | |
|---|---|---|
| 2140 | UDP | Deep Throat |
| 2155 | TCP | Illusion Mailer |
| 2222 | UDP | BackDoor.Botex |
| 2283 | TCP | Dumaru.Y |
| 2322 | TCP | backdoor.shellbot |
| 2333 | TCP | backdoor.shellbot |
| 2334 | TCP | Eyeveg.worm.c |
| 2335 | TCP | backdoor.shellbot |
| 2414 | TCP | vbs.shania |
| 2565 | TCP | Striker |
| 2583 | TCP | WinCrash |
| 2716 | TCP | The Prayer 1.2 -1.3 |
| 2721 | TCP | Phase Zero |
| 2745 | TCP | Beagle.J |
| 2766 | TCP | W32.hllw.deadhat.b |
| 2801 | TCP | Phineas Phucker |
| 2989 | TCP | Backdoor.Brador.A |
| 2989 | UDP | Rat |
| 3024 | TCP | WinCrash |
| 3028 | TCP | Backdoor.Wortbot |
| 3030 | TCP | W32.Mytob.cz@mm |
| 3067 | TCP | W32.korgo.a |
| 3127 | TCP | Trojans & Worms using this port |
| 3127 - 3198 | TCP | MyDoom.B@mm |
| 3129 | TCP | Master's Paradise |
| 3150 | TCP | Deep Throat |
| 3150 | UDP | Deep Throat |
| 3195 | TCP | Backdoor.IRC.Whisper.b |
| 3256 | TCP | W32.HLLW.Dax |
| 3306 | TCP | Backdoor.Nemog.D |
| 3332 | TCP | Trojans & Worms using this port |
| 3385 | TCP | w32.Mytob.kp@MM |
| 3737 | TCP | Backdoor.helios |
| 3410 | TCP | W32.mockbot.a.worm |
| 3456 | TCP UDP | Backdoor.Fearic |
| 3459 | TCP | Eclipse 2000 |

| | | |
|---|---|---|
| 3547 | TCP | Backdoor.Amitis.B |
| 3700 | TCP | Portal of Doom |
| 3791 | TCP | Eclypse |
| 3801 | UDP | Eclypse |
| 4000 | UDP | WityWorm (BlackICE/ISS) |
| 4001 | TCP | Backdoor.OptixPro.13.C |
| 4092 | TCP | WinCrash |
| 4128 | TCP | Backdoor.rcserv |
| 4242 | TCP | Backdoor.Nemog.D |
| 4300 | TCP | Backdoor.smokodoor |
| 4387 | TCP | Phatbot |
| 4444 | TCP | Trojans & Worms using this port |
| 4512 | TCP | W32.mytob.db |
| 4567 | TCP | File Nail |
| 4590 | TCP | ICQ Trojan |
| 4646 | TCP | Backdoor.Nemog.D |
| 4661 | TCP | Backdoor.Nemog.D |
| 4751 | TCP | Beagle.U |
| 4820 | TCP | Backdoor.tuxder |
| 4888 | TCP | W32.Opanki |
| 4899 | TCP | W32.RaHack |
| 4903 | TCP | Common Port for phishing scam sites |
| 8080 | TCP | Trojans & Worms using this port |
| 8081 | TCP | Trojans & Worms using this port |
| 9999 | TCP | The prayer 1.2 -1.3 |
| 5000 | TCP | Trojans & Worms using this port |
| 5001 | TCP | Sokets de Trois v1./Bubbel |
| 5011 | TCP | Ootlt |
| 5031 | TCP | Net Metropolitan 1.0 |
| 5032 | TCP | Net Metropolitan 1.04 |
| 5152 | TCP | Backdoor.laphex.client |
| 5190 | TCP | Trojans & Worms using this port |
| 5321 | TCP | Firehotcker |
| 5400 | TCP | Blade Runner |
| 5401 | TCP | Blade Runner |
| 5402 | TCP | Blade Runner |
| 5418 | TCP | Backdoor.DarkSky.B |

| | | |
|---|---|---|
| 5419 | TCP | Backdoor.DarkSky.B |
| 5503 | UDP | Remote Shell Trojan |
| 5521 | TCP | Illusion Mailer |
| 5550 | TCP | Xtcp |
| 5512 | TCP | Xtcp |
| 5553 | TCP | Backdoor.Xlog |
| 5554 | TCP | W32.Sasser.Worm |
| 5555 | TCP | Backdoor.Sysbug |
| 5555 | TCP | Backdoor.OptixPro |
| 5556 | TCP | BO Facil |
| 5557 | TCP | BO Facil |
| 5558 | TCP | Backdoor.Easyserv |
| 5569 | TCP | Robo-Hack |
| 5555 | TCP | W32.MiMail.P |
| 5588 | TCP | Backdoor.EasyServ |
| 5637 | TCP | PC Crasher |
| 5638 | TCP | PC Crasher |
| 5714 | TCP | WinCrash |
| 5741 | TCP | WinCrash |
| 5742 | TCP | WinCrash |
| 5800 | TCP | Backdoor.Evivinc |
| 5900 | TCP | Backdoor.Evivinc |
| 6000 | TCP | LovGate.ak |
| 6129 | TCP | W32.mockbot.a.worm |
| 6180 | TCP | Common Port for phishing scam sites |
| 6187 | TCP | Trojan.Tilser |
| 6400 | TCP | The Thing |
| 6565 | TCP | Backdoor.Nemog.D |
| 6631 | TCP | backdoor.sdbot.ag |
| 6667 | TCP | Trojans & Worms using this port |
| 6669 | TCP | Vampyre |
| 6670 | TCP | Deep Throat |
| 6671 | TCP | Deep Throat |
| 6711 | TCP | Sub Seven, Backdoor.G |
| 6712 | TCP | Sub Seven |
| 6713 | TCP | Sub Seven |
| 6723 | TCP | Mstream attack-handler |

| | | |
|---|---|---|
| 6771 | TCP | Deep Throat |
| 6776 | TCP | Sub Seven, Backdoor.G |
| 6777 | TCP | W32/Bagle@MM |
| 6789 | TCP | NetSky.U |
| 6838 | UDP | Mstream Agent-handler |
| 6912 | TCP | Sh*t Heap |
| 6939 | TCP | Indoctrination |
| 6969 | TCP | Trojans & Worms using this port |
| 6970 | TCP | Gate Crasher |
| 7000 | TCP | w32.mytob.mx@mm |
| 7043 | TCP | W32.Spybot.ycl |
| 7000 | TCP | Remote Grab |
| 7028 | TCP | Unknown Trojan |
| 7028 | UDP | Unknown Trojan |
| 7300 | TCP | Net Monitor |
| 7301 | TCP | Net Monitor |
| 7306 | TCP | Net Monitor |
| 7307 | TCP | Net Monitor |
| 7308 | TCP | Net Monitor |
| 7329 | TCP | Backdoor.netshadow |
| 7410 | TCP | Backdoor.phoenix |
| 7597 | TCP | QaZ (Remote Access Trojan) |
| 7614 | TCP | Backdoor.GRM |
| 7740 | TCP | backdoor.nodelm |
| 7741 | TCP | backdoor.nodelm |
| 7742 | TCP | backdoor.nodelm |
| 7743 | TCP | backdoor.nodelm |
| 7744 | TCP | backdoor.nodelm |
| 7745 | TCP | backdoor.nodelm |
| 7746 | TCP | backdoor.nodelm |
| 7747 | TCP | backdoor.nodelm |
| 7748 | TCP | backdoor.nodelm |
| 7749 | TCP | backdoor.nodelm |
| 7789 | TCP | ICKiller |
| 7823 | TCP | Backdoor.Amitis.B |
| 7955 | TCP | W32.kibuv.b |
| 7983 | UDP | MStream handler-agent |

| | | |
|---|---|---|
| 7999 | TCP | w32.mytob.lz@mm |
| 8000 | TCP | w32.mytob.jw@mm |
| 8012 | TCP | Backdoor.Ptakks.b |
| 8076 | TCP | W32.Spybot.pen |
| 8080 | TCP | Trojans & Worms using this port |
| 8090 | TCP | Backdoor.Asniffer |
| 8126 | TCP | W32.PejayBot |
| 8787 | TCP UDP | BackOrifice 2000 |
| 8811 | TCP | Backdoor.Monator |
| 8866 | TCP | Beagle.B@mm |
| 8879 | TCP UDP | BackOrifice 2000 |
| 8888 | TCP | W32.Axatak |
| 8889 | TCP | W32.Axatak |
| 9000 | TCP | W32.randex.ccf |
| 9125 | TCP | Backdoor.nibu.k |
| 9325 | UDP | MStream Agent-handler |
| 9400 | TCP | InCommand |
| 9604 | TCP | W32.kibuv.worm |
| 9696 | TCP | Backdoor.gholame |
| 9697 | TCP | Backdoor.gholame |
| 9870 | TCP | BackDoor.RC3.B |
| 9872 | TCP | Portal of Doom |
| 9873 | TCP | Portal of Doom |
| 9874 | TCP | Portal of Doom |
| 9875 | TCP | Portal of Doom |
| 9876 | TCP | Cyber Attacker |
| 9878 | TCP | Trans Scout |
| 9898-9999 | TCP | W32.dabber.a |
| 9989 | TCP | iNi-Killer |
| 9995 | TCP | W.32.Sasser Worm |
| 9999 | TCP | Trojans & Worms using this port |
| 10000 | TCP | W32.dumaru.ad |
| 10001 | TCP | Backdoor.Zdemon.126 |
| 10002 | TCP | Backdoor.Zdemon.126 |
| 10008 | TCP | Cheese worm |
| 10027 | TCP | w32.mytob.jw@mm |

| | | |
|---|---|---|
| 10067 | TCP | Portal of Doom |
| 10067 | UDP | Portal of Doom |
| 10080 | TCP | Mydoom.B |
| 10100 | TCP | backdoor.ranky.o |
| 10102 | TCP | backdoor.staprew |
| 10103 | TCP | backdoor.tuimer |
| 10167 | UDP | Portal of Doom |
| 10498 | UDP | Mstream handler-agent |
| 10520 | TCP | Acid Shivers |
| 10607 | TCP | Coma |
| 10666 | TCP | Ambush |
| 11000 | TCP | Senna Spy |
| 11050 | TCP | Host Control |
| 11223 | TCP | Progenic Trojan |
| 11768 | TCP | Dipnet / oddBob Trojan |
| 11831 | TCP | Latinus Server |
| 12000 | TCP | Backdoor.Satancrew |
| 12065 | TCP | Backdoor.Berbew.j |
| 12076 | TCP | GJamer |
| 12223 | TCP | Hack'99, KeyLogger |
| 12345 | TCP | Netbus, Ultor's Trojan |
| 12346 | TCP | Netbus |
| 12456 | TCP | NetBus |
| 12361 | TCP | Whack-a-Mole |
| 12362 | TCP | Whack-a-Mole |
| 12631 | TCP | Whack Job |
| 12701 | TCP | Eclypse 2000 |
| 12754 | TCP | Mstream attack-handler |
| 13000 | TCP | Senna Spy |
| 13173 | TCP | Backdoor.Amitis.B |
| 13468 | TCP | W32.Sober.D |
| 13700 | TCP | Kuang2 the Virus |
| 14247 | TCP | Trojan.Mitglieder.h |
| 15104 | TCP | Mstream attack-handler |
| 15118 | TCP | Dipnet / oddBob Trojan |
| 15432 | TCP | Backdoor.Cyn |
| 16322 | TCP | Backdoor.Lastdoor |

| | | |
|---|---|---|
| 16484 | TCP | Mosucker |
| 16661 | TCP | Backdoor.Haxdoor.D |
| 16959 | TCP | SubSeven DEFCON8 2.1 Backdoor |
| 16969 | TCP | Priority |
| 17300 | TCP | Kuang2.B Trojan |
| 17940 | TCP | W32.Imav.a |
| 18753 | UDP | Shaft handler to Agent |
| 19937 | TCP | Backdoor.Gaster |
| 20000 | TCP | Millennium |
| 20001 | TCP | Millennium |
| 20034 | TCP | NetBus 2 Pro |
| 20203 | TCP | Logged! |
| 20331 | TCP | Bla Trojan |
| 20432 | TCP | Shaft Client to handlers |
| 20433 | TCP | Shaft Agent to handlers |
| 20480 | TCP | Trojan.Adnap |
| 20742 | TCP | Trojan.Mitglieder.E |
| 21211 | TCP | W32.dasher.b |
| 21554 | TCP UDP | GirlFriend |
| 22222 | TCP | Prosiak |
| 22311 | TCP | Backdoor.Simali |
| 22784 | TCP | Backdoor-ADM |
| 23005 | TCP | W32.hllw.nettrash |
| 23006 | TCP | W32.hllw.nettrash |
| 23232 | TCP | backdoor.berbew.j |
| 23435 | TCP | Trojan.Framar |
| 23476 | TCP | Donald Dick |
| 23477 | TCP | Donald Dick |
| 23523 | TCP | w32.mytob.km@mm |
| 2556 | TCP | Beagle.N |
| 26274 | TCP | Delta Source |
| 26274 | UDP | Delta Source |
| 27015 | UDP | linux.plupii.c |
| 27374 | UDP | Sub-7 2.1 |
| 27379 | TCP | Backdoor.optix.04 |
| 27444 | UDP | Trin00/TFN2K |
| 27573 | UDP | Sub-7 2.1 |

| | | |
|---|---|---|
| 27573 | TCP | Sub-7 2.1 |
| 27665 | TCP | Trin00 DoS Attack |
| 29147 | TCP | Backdoor.Sdbot.ai |
| 29292 | TCP | Backdoor.NTHack |
| 29559 | TCP | Latinus Server |
| 29891 | TCP | The Unexplained |
| 29999 | TCP | Backdoor.Antilam.20 |
| 30029 | TCP | AOL Trojan |
| 30100 | TCP | NetSphere |
| 30101 | TCP | NetSphere |
| 30102 | TCP | NetSphere |
| 30133 | TCP | NetSphere Final |
| 30303 | TCP | Sockets de Troi |
| 30999 | TCP | Kuang2 |
| 31335 | UDP | Trin00 DoS Attack |
| 31336 | TCP | BO-Whack |
| 31337 | UDP | Backorifice (BO) |
| 31337 | TCP | Netpatch |
| 31338 | TCP | NetSpy DK |
| 31338 | UDP | Deep BO |
| 31339 | TCP | NetSpy DK |
| 31666 | TCP | BOWhack |
| 31785 | TCP | Hack'a'Tack |
| 31787 | UDP | Hack`a'Tack |
| 31789 | UDP | Hack'a'Tack |
| 31790 | UDP | Hack`a'Tack |
| 31791 | UDP | Hack'a'Tack |
| 32121 | TCP | backdoor.berbew.j |
| 32418 | TCP | Acid Battery |
| 32440 | TCP | Backdoor.Alets.B |
| 33270 | TCP | Trinity Trojan |
| 33322 | TCP | trojan.lodeight.b |
| 33333 | TCP | Prosiak |
| 33911 | TCP | Spirit 2001 a |
| 34324 | TCP | BigGluck, TN |
| 36183 | TCP | Backdoor.Lifefournow |
| 37651 | TCP | Yet Another Trojan |

| | | |
|---|---|---|
| 39999 | TCP | TrojanProxy.Win32.Mitglieder |
| 40421 | TCP | Master's Paradise |
| 40412 | TCP | The Spy |
| 40421 | TCP | Agent, Master's of Paradise |
| 40422 | TCP | Master's Paradise |
| 40423 | TCP | Master's Paradise |
| 40425 | TCP | Master's Paradise |
| 40426 | TCP | Master's Paradise |
| 43210 | TCP | Master's Paradise |
| 44280 | TCP | Backdoor.Amitis.B |
| 44390 | TCP | Backdoor.Amitis.B |
| 47252 | TCP | Delta Source |
| 47262 | UDP | Delta Source |
| 47387 | TCP | Backdoor.Amitis.B |
| 47891 | TCP | Backdoor.antilam.20 |
| 49301 | UDP | OnLine keyLogger |
| 50005 | TCP | Trojan.Fulamer.25 |
| 50505 | TCP | Sokets de Trois v2. |
| 50776 | TCP | Fore |
| 51234 | TCP | Backdoor.Cyn |
| 51435 | TCP | W32.kalel.a@mm |
| 53001 | TCP | Remote Windows Shutdown |
| 54320 | TCP | Back Orifice 2000 |
| 54320 | UDP | Back Orifice |
| 54321 | TCP | School Bus, Back Orifice |
| 54321 | UDP | Back Orifice 2000 |
| 56565 | TCP | Backdoor.Osirdoor |
| 57341 | UDP | NetRaider Trojan |
| 57341 | TCP | NetRaider Trojan |
| 58008 | TCP | BackDoor.Tron |
| 58009 | TCP | BackDoor.Tron |
| 58666 | TCP | BackDoor.Redkod |
| 59211 | TCP | BackDoor.DuckToy |
| 60000 | TCP | Deep Throat |
| 60006 | TCP | Trojan.Fulamer.25 |
| 61000 | TCP | Backdoor.mite |
| 61466 | TCP | Telecommando |

| | | |
|---|---|---|
| 61348 | TCP | Bunker-Hill Trojan |
| 61603 | TCP | Bunker-Hill Trojan |
| 63485 | TCP | Bunker-Hill Trojan |
| 63808 | TCP | Phatbot |
| 63809 | TCP | Phatbot |
| 63809 | TCP | W32.hllw.gaobot.dk |
| 64429 | TCP | Backdoor.Amitis.B |
| 65000 | TCP | Trojans & Worms using this port |
| 65506 | TCP | Phatbot |
| 65535 | TCP | Adore Worm/Linux |