

## Re: Recycler security issues on IIS server

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.inetserver.iis.security/2002-10/5433.html>

---

**From:** Karl Levinson [x y] mvp ([levinson\\_k@excite.com](mailto:levinson_k@excite.com))

**Date:** 10/30/02

From: "Karl Levinson [x y] mvp" <[levinson\\_k@excite.com](mailto:levinson_k@excite.com)>

Date: Wed, 30 Oct 2002 12:21:20 -0500

"Matthew" <[mjaremko@preferredone.com](mailto:mjaremko@preferredone.com)> wrote in message  
news:c78b01c28027\$d84cd8f0\$39ef2ecf@TKMSFTNGXA08...

- > *One of our webservers that sits outside a firewall*
- > *recently was compromised. In the recycler folder we*
- > *discovered a nest of folders that contained DVD images,*
- > *hacked games, etc. We deleted the files and applied the*
- > *latest updates to the server.*
- >
- > *Is cleaning up the folder and applying the latest patches*
- > *enough? Should more steps be taken? I personally would*
- > *like to see the server put behind our firewall, but this*
- > *is unlikely to happen.*

Whyever would you have any machines outside of your firewall? IMHO this is a terrible idea. Firewalls are very cheap nowadays, like the [www.netscreen.com](http://www.netscreen.com) 5XP for \$500 US or a free Linux / BSD boot CD firewall on an old 486 PC such as IPcop, Gibraltar, Smoothwall, ClosedBSD, etc. Even [www.sygate.com](http://www.sygate.com) software is free for non-commercial use. Without a firewall or router that is doing logging, you've got absolutely no proof or evidence to track or prosecute a hacker. That's very bad.

The answer to your question depends on your individual security needs. If you want to be 100% sure you've removed all the back doors from the server and it won't be hacked again, you need to format, reinstall windows and all other software, install all patches, IISlockdown, URLscan, use the correct configuration by following several hardening checklists [ [www.microsoft.com/technet/security](http://www.microsoft.com/technet/security), [www.nsa.gov](http://www.nsa.gov), <http://rr.sans.org>, etc.] and put it behind a firewall. Note that installing patches is not enough, you also need to configure your system securely. You can also run vulnerability assessment scanners starting with MBSA which is free from [www.microsoft.com/download](http://www.microsoft.com/download)

You can if you wish just try to remove what you can find, but there's no guarantee that you'll remove everything. Before you format or delete files, you also want to inspect the logs and evidence on the machine to determine how the hack was done to confirm that that vulnerability has been closed and

that other machines are not also compromised.

This type of hack could have been something as benign as someone finding that your FTP server allowed the anonymous account to both read and write to the same folder [this is bad, but is not as bad as other hacks]. However, if you left your server configured this way, there are probably other more serious vulnerabilities, and your server could very well have been compromised other times that you don't know about.

I definitely wouldn't move it behind the firewall without formatting. Check the IIS web and FTP server logs for some evidence, and run vision from [www.foundstone.com/knowledge](http://www.foundstone.com/knowledge), an antivirus and trojan scanner such as Norton and [www.pestpatrol.com](http://www.pestpatrol.com), etc. [www.network-tools.com](http://www.network-tools.com) and <http://visualroute.visualware.com> will help you look up the IP address in your logs to know which ISP to complain to. Also check out the Languard File Integrity Checker [URL below] and [www.mynetwatchman.com](http://www.mynetwatchman.com)

If this is a company, you may also want to consider reporting this to the FBI or the local authorities in your country. They probably won't prosecute unless you have demonstrable financial loss from the event, but they or the local police may be interested anyways. Without the IP address of the attackers, though, you've got nothing.

Read below for some further information and other steps that I would highly recommend.

=====

How can I tell if I've been hacked?

A: This can be a complicated procedure and usually requires both prior experience with forensic investigations and knowledge of what the computer looked like [which files existed, which ports were open, etc.] or what a similar computer looks like before being compromised.

Also, the procedures you follow may vary depending on your security needs. For example, performing some of the procedures below may modify the files on your computer so that it is not admissible as evidence in court. Other procedures below could alert a hacker to the fact that you are looking for her, causing her to delete evidence or retaliate against you in some way.

If this is a business computer, your company should seriously consider hiring a security consultant or contacting the appropriate local law enforcement agency, both for the initial forensic response and also to improve your security to avoid future intrusions.

Keep in mind during the investigation that this might NOT be a hacker intrusion and might instead be regular network activity or a worm. Books such as Incident Response, Hacker's Challenge and/or Hacking Exposed 3rd Edition may offer you more information on how to investigate intrusions.

You may consider performing the actions below:

1. Unplugging the network cable is one possible way to try to prevent further damage.
2. Use Fport or Vision from [www.foundstone.com/knowledge](http://www.foundstone.com/knowledge) or pslist / pstools from [www.sysinternals.com](http://www.sysinternals.com) to look at the open ports on your computer and the program or executable using that port. Some firewall software such as [www.sygate.com](http://www.sygate.com) will also tell you this information.

You can also use the NETSTAT -A command that comes with Windows to look at open ports; however, this will not identify which program is using the port.

If you're unsure about the purpose of a particular port or program, try searching an Internet search engine such as [www.google.com](http://www.google.com) for the name of the port or program, or try right-clicking on the file in question to see the properties. Or, you could even try to telnet to that port e.g. by typing TELNET LOCALHOST PORTNUMBER or TELNET COMPUTERTNAME PORTNUMBER [example, TELNET LOCALHOST 82 ] and press the Enter key a few times to see if any informative messages appear.

3. Consider using a file change checker, such as the unsupported free tool Languard File Integrity Checker at [www.gfi.com/languard/lantools-fic.htm](http://www.gfi.com/languard/lantools-fic.htm). Recently changed files on your system can sometimes indicate an intrusion. You could also find and list the files on your hard drives that have been modified in the past 3 days by clicking on Start, Search [or Find], Files or Folders, and setting the appropriate date [though note that this may change the "Last Accessed" date stamp on some of these files]. "The Forensic Toolkit" from [www.foundstone.com/knowledge](http://www.foundstone.com/knowledge) includes command-line tools to list files without modifying the date.

4. Inspect the programs that launch when Windows starts on your computer, by using MSCONFIG or Startup Cop. Suspicious programs starting when Windows starts can indicate a successful intrusion. [These can also indicate less serious events such as a virus or worm infection or even the installation of a freeware or ad-ware program such as an MP3 music file-sharing program.] See the section in this FAQ entitled "I think there may be a suspicious program, Trojan, ad-ware, "porn dialer," etc. starting up on my computer when Windows starts" for more information on how to do this.

5. Check the logs on your computer, especially your Internet router or firewall logs, the IIS web and ftp server logs and Windows security event log. [This is probably the first thing to do if IIS web services are running on the computer.] Some of these logs may not exist if you have not already enabled them.

Many common hacks are first seen in the IIS web server logs. Any line in your web server log that contains % or .EXE and which also contains a 200 or 502 error code is cause for further investigation. If you are familiar with DOS commands, you may be able to see exactly what commands the intruder tried to execute. Keep in mind that every web server on the Internet will

have suspicious looking entries from worms like Nimda, though these are not necessarily signs of a successful intrusion.

For more information on deciphering web server logs, see the section in this FAQ entitled "I keep seeing strange things in my IIS web server logs, like 'NNNNNNNNNN' or 'GET /scripts/root.exe' Have I been hacked?"

6. Consider using a Trojan scanner. Antivirus programs generally detect some but not all of the most common Trojans and hacker tools. Some people choose to use a Trojan scanner in addition to antivirus.

For more information on where and how to locate and use free and not-free Trojan scanner software, see the section in this FAQ entitled "Which antivirus should I choose? Which antivirus is the best?"

7. Consider installing an antivirus program that is configured to automatically download updates daily.

For more information on where and how to locate and use free and not-free antivirus software, see the section in this FAQ entitled "Which antivirus should I choose? Which antivirus is the best?"

8. Consider running a port scanner [and/or a vulnerability scanner] to look for security flaws and configuration errors on your computers. For example, you might also run a port scanner against your computers to look for open ports. A particular open port might indicate the way a hack occurred and/or might give you a way to identify other infected computers. Begin with Vision, Fport and/or SuperScan from [www.foundstone.com/knowledge](http://www.foundstone.com/knowledge), MBSA from [www.microsoft.com/download](http://www.microsoft.com/download) and/or Languard Network Scanner from [www.gfi.com](http://www.gfi.com)

See the section in this FAQ entitled "How can I scan my computer or firewall to look for open ports or confirm that my machine is secure?" for more information.

9. Consider enabling or installing a firewall and/or a sniffer [either software or hardware based] to monitor and look for unusual network traffic. There are a number of free firewalls available on the Internet which can show network transmissions to and from your computer, such as [www.sygate.com](http://www.sygate.com), or you could use the Network Monitor which comes with Windows 2000 / XP / NT / .NET, or Ethereal at [www.ethereal.com](http://www.ethereal.com), or Windump at <http://windump.polito.it>

For more information on how and where to locate free and not-free firewall software and hardware, see the section in this FAQ entitled "Which firewall should I choose? Which firewall is the best?"

10. The third party web sites and tools below may also be helpful:

[www.sysinternals.com](http://www.sysinternals.com)

For example, some of the helpful free tools on this site include Filemon, Regmon and Process Explorer which all display activity on your computer you might not otherwise be able to see. These tools show which files, registry keys, .DLLs and other objects are currently being accessed and by which process.

Pstools is a group of tools including pslist, which lists detailed information about processes, and psloggedon, which displays who is logged onto your computer currently.

[www.foundstone.com/knowledge](http://www.foundstone.com/knowledge)

In addition to the Vision / Fport tools, one of the free tools on this site is NTLast, a security event log analysis tool that helps identify who has gained access to the system, using the NT security event logs [assuming auditing has previously been turned on].

Also, the Forensic Toolkit is a collection of tools including:

- \* Afind, which lists recently accessed files without changing the date stamp on the file;
- \* Hfind, which scans the disk for hidden files;
- \* Sfind, which scans the disk for files hidden in data streams.

[www.incident-response.org/IRCR.htm](http://www.incident-response.org/IRCR.htm)

Incident Response Collection Report (IRCR) is a collection of forensic tools that automates many of the tasks a forensics expert might perform.

If you have trouble understanding the results of any of these tools, you can post your results along with your question to an appropriate Usenet newsgroup. Note that the Microsoft newsgroups may not be the place to get the best answers to your questions, though you can try and see what happens.

[Thanks to Susan Bradley, Rob Lee and others]

=====

How can I harden my computer or server to secure it from hackers?

A: [Note that if you have already been hacked, this section will not help you re-secure your computer. In this case, you should first read the section in this FAQ entitled "How can I re-secure my computer or server after being hacked?"]

Here is the short answer:

1. Do not put the computer onto the network or the Internet until after the computer has been hardened using the instructions below [or at least not before a firewall and antivirus have been installed].
2. Use firewall software and hardware and antivirus software that is configured to download updates every day;

3. Follow the instructions for hardening Windows and IIS at [www.microsoft.com/technet/security](http://www.microsoft.com/technet/security) ;
4. Install all service packs and security fixes from Microsoft and otherwise for all Microsoft software on your computer [Windows, IIS, Office, Internet Explorer, Windows Media Player, etc.] from [www.microsoft.com/technet/security](http://www.microsoft.com/technet/security) ;
5. [Ongoing] Download MBSA from [www.microsoft.com/download](http://www.microsoft.com/download) and run it now and also at regular intervals to look for vulnerabilities in your settings, new patches that are missing, etc. Also, check your antivirus to confirm that the last successful update was less than 14 days ago.

These steps will make your computer fairly secure, but may still leave some holes. Keep reading below for additional information you should be aware of:

A successful hacker, virus or worm intrusion into one of your computers can drain your free disk space, slow down your Internet connection, compromise your credit card numbers, damage your personal documents, allow intruders to access other machines on your network that DO contain important files, and/or leave you legally liable for other government or business computers on the Internet that are hacked by an intruder using your computer. This is why you should consider securing ALL the computer systems in your home or network, even if you think there is nothing important on the computer or it is "just a test computer."

All Windows users should seriously consider all of the procedures below to help prevent intrusions on their computers:

1. Do not put the computer onto the network or the Internet until after the computer has been hardened using the instructions below. [Un-secured computers can be hacked in just 15 minutes or less after being put onto the Internet.] Depending on your environment, it may be acceptable to put your computer on the Internet after installing a firewall and antivirus software with the latest updates.
2. Seriously consider enabling or installing firewall software and/or firewall hardware. There are a number of free firewalls available, including the ICF feature that comes with Windows XP [unless XP is joined to a Windows domain], and/or other third-party firewalls available on the Internet.

For more information on how and where to locate free and not-free firewall software and hardware, see the section in this FAQ entitled "Which firewall should I choose? Which firewall is the best?"

3. Seriously consider installing an antivirus program and configure it to automatically download updates daily.

For more information on where and how to locate and use free and not-free antivirus software, see the section in this FAQ entitled "Which antivirus should I choose? Which antivirus is the best?"

4. Follow the instructions for hardening Windows 2000 and also IIS [if IIS is installed] at [www.microsoft.com/technet/security](http://www.microsoft.com/technet/security) [For Windows 2000 / NT, hardening IIS usually includes installing IISlockdown including URLScan. For computers with FTP service installed, it usually includes removing the Posix subsystem and removing write permission from the anonymous user account, among other things.]

5. Download and install all the service packs and security patches from [www.microsoft.com/technet/security](http://www.microsoft.com/technet/security) for all the Microsoft and non-Microsoft software installed on your computer, especially Microsoft Windows, Office, Internet Explorer, Outlook Express, Windows Media Player and IIS [if IIS is installed].

Note that Windows 2000, XP, .NET and NT users should also download patches for Indexing Services a.k.a. Index Server. Do not assume that Index Server patches are included with any IIS comprehensive service pack rollup you may already have installed, because they are not.

[If you want a shortcut to do this faster, you could try this:

- \* Download and install the latest Windows service pack from [www.microsoft.com/technet/security](http://www.microsoft.com/technet/security);

- \* Reboot and visit <http://windowsupdate.microsoft.com> to receive additional patches;

- \* Reboot, download and run MBSA [Microsoft Baseline Security Analyzer] or HFNETCHK from [www.microsoft.com/download](http://www.microsoft.com/download) to discover other missing patches;

- \* Manually download from [www.microsoft.com/technet/security](http://www.microsoft.com/technet/security) and install any patches that were found to be missing, as well as patches for any server products that may not be included in Windows Update and MBSA/HFNETCHK, such as possibly SQL Server, ISA Server, etc.

- \* NOTE however that Windows Update, MBSA and HFNETCHK do NOT necessarily list all Microsoft patches or search all Microsoft products, so you could be missing some patches if you rely just on these tools.]

6. [ONGOING] Re-run the MBSA tool from [www.microsoft.com/download](http://www.microsoft.com/download) every 60 days or sooner to look for missing patches, and confirm that your antivirus program received an update in the past 10 days or less.

If you want or need even more security [or are particularly paranoid or at risk], you can consider some of the additional steps below. Some of the tools below may be more security than you need, unless you are running a server such as IIS web or FTP services.

- \* Download and install MyNetWatchman or Dshield. These are free programs that work with your firewall software or hardware to automatically report hacking attempts to the hacker's ISP. You get to see information about whether that IP address has been used to scan or hack other computers, or whether it might be targeting just your computer. You also get to see whether the ISP has responded or taken action against the offending user. This is highly recommended. You can get this software at one of the links below:

www.mynetwatchman.com  
www.dshield.org

\* Sign up for the Microsoft security mailing list at [www.microsoft.com/technet/security](http://www.microsoft.com/technet/security) to receive emails with a link to new critical security patches as they are released, and install them ASAP.

\* Use Fport or Vision from [www.foundstone.com/knowledge](http://www.foundstone.com/knowledge) or pslist / pstools from [www.sysinternals.com](http://www.sysinternals.com) to look at the open ports on your computer and the program or executable using that port. Some firewall software such as [www.sygate.com](http://www.sygate.com) will also tell you this information.

You can also use the NETSTAT -A command that comes with Windows to look at open ports; however, this will not identify which program is using the port.

[You may want to run a command such as FPORT >> C:\OPENPORTS.TXT or PSLIST >> C:\OPENPORTS.TXT or NETSTAT -A >> C:\OPENPORTS.TXT This command will create a "baseline" text file named c:\openports.txt that can be compared later with the results of the command to tell you whether additional ports are now open, a possible sign of intrusion.]

\* Consider running one or more vulnerability scanners to look for security flaws and configuration errors on your computers. Vulnerability scanners should be run after you have installed and hardened a new computer or server, and also run at regular intervals to confirm that your computers are still secure. You might also run a port scanner against your computers as well to look for open ports.

See the section in this FAQ entitled "How can I scan my computer or firewall to look for open ports or confirm that my machine is secure?" for more information.

\* Consider searching for and following additional checklists for hardening Windows 2000 by searching an Internet search engine such as [www.google.com](http://www.google.com) for words such as "harden OR hardening windows-2000" [e.g. [www.google.com/search?q=harden+OR+hardening+windows-2000](http://www.google.com/search?q=harden+OR+hardening+windows-2000) ]. Several such checklists are available at <http://nsa1.www.conxion.com/win2k/download.htm> a.k.a. <http://www.nsa.gov>, as well as [www.labmice.net/security](http://www.labmice.net/security), <http://rr.sans.org>, etc.

\* Uninstall any unnecessary Windows components [e.g. click on Start, Settings, Control Panel, Add/Remove Programs, Add/Remove Windows Components]. Pay particular attention to Indexing Service, Internet Information Services (IIS), Management and Monitoring Tools, Message Queuing Services, Networking Services, Other Networking File and Print Services, Outlook Express, and Windows Media Player. If you are not sure whether something is unnecessary, try searching [www.google.com](http://www.google.com) or posting a question to the appropriate Microsoft security newsgroup.

\* Disable any unnecessary Windows services [e.g. click on Start, Settings, Control Panel, Administrative Tools, Services]. If you are not sure whether

something is unnecessary, try searching [www.google.com](http://www.google.com) or posting a question to the appropriate Microsoft security newsgroup.

\* Consider using a Trojan scanner. Antivirus programs generally detect some but not all of the most common Trojans and hacker tools. Some people choose to use a Trojan scanner in addition to antivirus.

For more information on where and how to locate and use free and not-free Trojan scanner software, see the section in this FAQ entitled "Which antivirus should I choose? Which antivirus is the best?"

\* Enable logging. Most logging is disabled by default, and usually this is not discovered until after an intrusion, when the logs are needed.

Enable logging of your IIS web server, FTP server, etc. For sites with a small number of hits, consider changing logs to rotate monthly instead of daily to allow easier searching of logs.

Enable logging on your Internet router, switch or firewall. [Because these devices usually do not have much storage space for saving logs, doing this may involve installing free syslog software onto your computer to be able to capture the logs.]

Enable auditing of security events on your Windows system, including logon successes and/or failures and NTFS auditing of files and registry keys. For more information, see the section in this FAQ entitled "How can I enable auditing / logging on my computer / server?"

Change the Windows event log settings to be appropriate for your environment. Consider increasing the maximum log size to retain more information. Be careful not to log too much, or you might find that your logs contain only a few minutes or hours worth of data.

Check the logs to be sure logs are really being captured.

\* Consider using a file change checker, such as the unsupported free tool Languard File Integrity Checker at [www.gfi.com/languard/lantools-fic.htm](http://www.gfi.com/languard/lantools-fic.htm). Files changing on your system can sometimes indicate a hacker intrusion.

\* Consider using a Windows event log monitor. Some types of intrusions leave entries in one of the logs on your computer. [On an especially vulnerable or secure system, you should be sure that you've configured logging to detect events such as intrusions.] Some network monitors such as [www.ipsentry.com](http://www.ipsentry.com) can send a message to your email/screen/pager if a server or service stops responding, an event or error appears in a Windows log, etc. Windows log monitors can be found by searching an Internet search engine or your favorite software web site, or by using the links below:

[www.ipsentry.com](http://www.ipsentry.com) [around \$100 US]  
[www.sunbelt-software.com](http://www.sunbelt-software.com)  
[www.webattack.com](http://www.webattack.com)

[www.wilders.org](http://www.wilders.org)  
[www.download.com](http://www.download.com)  
[www.tucows.com](http://www.tucows.com)  
[www.google.com/search?q=windows+event+log+monitor](http://www.google.com/search?q=windows+event+log+monitor)

\* Consider using EFS file encryption [under Windows 2000 / XP / .NET] or third-party utilities to encrypt the files on your computer may be something to consider. Some of these utilities can encrypt your entire hard drive including Windows, whereas other tools just encrypt some of your data files and are not suitable for encrypting or preventing access to Windows.

Note that using any form of encryption can slow down your computer's performance. Also, you must be extremely careful to back up and protect your encryption key and any passwords. If the encryption keys are not backed up, users can lose their encrypted files forever when Windows is reinstalled, Windows encounters a problem so that Windows no longer starts up, etc.

For more information on EFS file encryption on Windows 2000 / XP / .NET, see the section in this FAQ entitled "I used Windows 2000 / XP EFS file encryption to encrypt some files. Now, I can't read the files. How can I unencrypt them or recover the key?"

Third party encryption software can be found at the following locations:

[www.pgp.com](http://www.pgp.com)  
[www.scramdisk.clara.net](http://www.scramdisk.clara.net)  
[www.e4m.net](http://www.e4m.net)  
[www.jetico.com](http://www.jetico.com) ["BestCrypt"]  
[www.download.com](http://www.download.com)  
[www.tucows.com](http://www.tucows.com)  
[www.google.com](http://www.google.com)

=====