

Re: been hit by hacker, servudaemon installed

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.inetserver.iis.security/2002-10/5321.html>

From: Karl Levinson [x y] MVP (jamescagney90210@excite.com)

Date: 10/27/02

From: "Karl Levinson [x y] MVP" <jamescagney90210@excite.com>

Date: Sun, 27 Oct 2002 07:08:41 -0500

If you're confident that the computer is secure [and you might be right] and all you want to do is to harden your computer, check out the section in my previous post titled "how do I harden or secure my computer..." Especially install all service packs and patches from Microsoft, follow the IIS and Windows 2000 hardening checklists from www.microsoft.com/technet/security and the other locations listed in my post including www.nsa.gov and <http://rr.sans.org> etc, make sure anonymous FTP is disabled or does not have write permission or at least does not have both read and write permission to any one folder, install IISlockdown including URLscan from www.microsoft.com/download, sign up for the Microsoft newsletter for notification of new security patches at www.microsoft.com/technet/security, disable the Posix subsystem, use antivirus and a file change checker such as the Languard file integrity checker [URL given in my previous post], use one of the firewalls and antivirus programs [even the free ones] listed in my previous post, etc.

"billemary" <emery_bill@hotmail.com> wrote in message news:f7cb01c27d68\$40198400\$3aef2ecf@TKMSFTNGXA09...

> reviewed logs, and deleted all warez content from
> harddrive, this was a comercial hack, using the harddrive
> at night for warez storage eg mp3's etc. via serudaemon.
> pretty ingenious actually, using the echo command to
> create the ftp.txt file, then running ftp using the
> ftp.txt file to get servudaemon on the harddrive.
> ive attached the section of the log file that shows what
> they did.
> all i want to do now is secure iis from this.
> what do i do ?
>
>
>
>
>
>
>
>
>
> >-----Original Message-----

microsoft.public.inetsrvr.iis.security: Re: been hit by hacker, servudaemon installed

>>
>> "BILLEMERY" <emery_bill@hotmail.com> wrote in message
>> news:77f801c27c41\$3a7108c0\$39ef2ecf@TKMSFTNGXA08...
>>>
> GET /scripts/test.exe /c+move+ServUDaemon.ini+c:\Inetpub\ii
>>> ssamples\sdk\asp\docs\help\system\drivers\dll 502 0
>>> 374344 (compatible;+MSIE+6.0;+Windows+NT+5.0)
>>>
>>> is one of the commands in my w3svc1 log files that got
> my
>>> attention. ive been hacked. this is unreal that anyone
> can
>>> use a sever by default to ftp a program to it.
>>
>>This is a pretty common attack.
>>
>>Every single one of the web servers and internet server
> operating systems
>>out there currently requires you to take steps to secure
> it. Linux,
>>Windows, Apache, you name it. No one except maybe
> OpenBSD has a secure
>>default install yet.
>>
>>Your computer may have been hacked into, in which case
> you may not be 100%
>>secure unless you format and reinstall windows and
> everything else and then
>>secure the machine. It's hard to tell without previous
> technical experience
>>in this.
>>
>>Before you format, however, you should probably
> investigate to see what was
>>done and why and whether other machines were
> compromised. If the hack went
>>through an unpatched bug in IIS web services, you should
> see exactly what
>>commands they entered in your IIS server logs. It could
> also be that you've
>>been hacked other times as well. Other tools you should
> use include Vision
>>from www.foundstone.com/knowledge, a trojan scanner such
> as
>>www.pestpatrol.com, etc. I recommend a file change
> checker such as the free
>>Languard File Integrity Checker from www.gfi.com [full
> URL listed below].
>>
>>It sounds like you haven't installed all the latest
> patches from Microsoft

Re: been hit by hacker, servudaemon installed

microsoft.public.inetsrvr.iis.security: Re: been hit by hacker, servudaemon installed

> >and haven't configured your machine using the variety of
> hardening checklist
> >instructions out there, this should be done as well after
> you format your
> >machine. [You can certainly choose not to format your
> machine, the choice
> >is up to you and your security needs.] It also sounds
> like you aren't
> >running IISlockdown including URLscan which would have
> also probably
> >prevented this attack. Free from
> www.microsoft.com/download or
> >www.microsoft.com/technet/security [get MBSA at the same
> time for free to
> >look for missing patches and other vulnerabilities on
> your server and other
> >computers on your network].
> >
> >More information on how to tell if you've been hacked,
> how to secure your
> >machine, where to get a firewall and antivirus program
> are all below:
> >
> >=====

> >
> >How can I tell if I've been hacked?
> >
> >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
> or pslist / pstools
> >from 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 will also tell you this information.
> >
> >You can also use the NETSTAT -A command that comes with

Re: been hit by hacker, servudaemon installed

microsoft.public.inetserver.iis.security: Re: been hit by hacker, servudaemon installed

> *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 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.*
> >*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 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*

Re: been hit by hacker, servudaemon installed

> *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
> >'NNNNNNNNN' 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

microsoft.public.inetsrv.iis.security: Re: been hit by hacker, servudaemon installed

> >antivirus software, see the sections in this FAQ
> entitled "Which antivirus
> >should I choose? Which antivirus is the best?" and the
> section entitled "I
> >think I might have a virus / worm / Trojan."
> >
> >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, MBSA from
> >www.microsoft.com/download and/or Languard Network
> Scanner from 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, or you could use the Network Monitor
> >which comes with
> >Windows 2000 / XP / NT / .NET, or Ethereal at
> >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

Re: been hit by hacker, servudaemon installed

microsoft.public.inetsrvr.iis.security: Re: been hit by hacker, servudaemon installed

> >
> >*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*
> >
> >*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*
> >
> >*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.*

Re: been hit by hacker, servudaemon installed

microsoft.public.inetsrvr.iis.security: Re: been hit by hacker, servudaemon installed

> >
> >[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 ;
> >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 ;
> >5. [Ongoing] Download MBSA from
> >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

Re: been hit by hacker, servudaemon installed

microsoft.public.inetsrv.iis.security: Re: been hit by hacker, servudaemon installed

> *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*

Re: been hit by hacker, servudaemon installed

microsoft.public.inetsrvr.iis.security: Re: been hit by hacker, servudaemon installed

> *free and not-free*
> >*antivirus software, see the sections in this FAQ*
> >*entitled "Which antivirus*
> >*should I choose? Which antivirus is the best?" and the*
> >*section entitled "I*
> >*think I might have a virus / worm / Trojan."*
> >
> >*4. Follow the instructions for hardening Windows 2000 and*
> >*also IIS [if IIS*
> >*is installed] at 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 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;*
> >** 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 to discover*
> >*other missing patches;*
> >** Manually download from*
> >*www.microsoft.com/technet/security and install any*

Re: been hit by hacker, servudaemon installed

microsoft.public.inetsrvr.iis.security: Re: been hit by hacker, servudaemon installed

> >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 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 to receive emails with
> a link to new
> >critical security patches as they are released, and
> install them ASAP.
> >

Re: been hit by hacker, servudaemon installed

microsoft.public.inetsrvr.iis.security: Re: been hit by hacker, servudaemon installed

> > * Use Fport or Vision from www.foundstone.com/knowledge
> or *pslist / pstools*
> > from 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 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
> > for words such as "harden OR hardening windows-2000" [e.g.
> > [www.google.com/search?q=harden+OR+hardening+windows-](http://www.google.com/search?q=harden+OR+hardening+windows-2000)
> > 2000]. Several such
> > checklists are available at
> > <http://nsa1.www.conxion.com/win2k/download.htm>

Re: been hit by hacker, servudaemon installed

microsoft.public.inetserver.iis.security: Re: been hit by hacker, servudaemon installed

- > >a.k.a. <http://www.nsa.gov>, as well as
- > 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 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 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.
- > >

microsoft.public.inetsrv.iis.security: Re: been hit by hacker, servudaemon installed

> >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
> >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.ipseentry.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.ipseentry.com [around \$100 US]
> >www.sunbelt-software.com

Re: been hit by hacker, servudaemon installed

microsoft.public.inetsrvr.iis.security: Re: been hit by hacker, servudaemon installed

> >www.webattack.com
> >www.wilders.org
> >www.download.com
> >www.tucows.com
> >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
> >www.scramdisk.clara.net
> >www.e4m.net
> >www.jetico.com ["BestCrypt"]
> >www.download.com
> >www.tucows.com
> >www.google.com
> >

> >
> >Which antivirus should I choose?
> >
> >The best way to deal with any virus on any computer or*

Re: been hit by hacker, servudaemon installed

> server is ALWAYS to
> >install and use an antivirus program that is updated with
> the latest updates
> >for that week [or day].
> >
> >Some antivirus manufacturers may release mini-tools that
> will remove a
> >particular virus or worm, such as a Nimda virus removal
> tool. However, these
> >single-virus removal tools generally do nothing to
> protect you from becoming
> >re-infected when you receive another infected email or
> file five minutes
> >after you ran the tool. Antivirus software is necessary
> to prevent against
> >re-infection and damage to your computer files.
> >
> >Just running an antivirus program is not enough. You
> should make sure that
> >your antivirus program can be configured to download
> updates every day [or
> >every week] automatically via the Internet, and open the
> program from time
> >to time to ensure that it is still receiving updates.
> >
> >NOTE however that if an antivirus scanner or Trojan
> scanner finds a Trojan
> >installed and running on your computer, it could be a
> sign of a hacker
> >intrusion, in which case you will want to consider taking
> additional steps
> >before removing the Trojan. For more information, see the
> section in this
> >FAQ entitled "How can I tell if I've been hacked?"
> >
> >If you have a particular file name and wish to find out
> whether or not it is
> >a virus [or a worm, a Trojan, a hoax, etc.], you can try
> searching an
> >Internet search engine such as www.google.com for that
> file name. However,
> >it is still best to install and use an antivirus scanner.
> Looking up a
> >particular file name is NOT a reliable way to determine
> whether or not the
> >file is a virus.
> >
> >Deleting a file from your system is never the first way
> or the best way to
> >try to remove a virus from your computer.
> >

microsoft.public.inetsrv.iis.security: Re: been hit by hacker, servudaemon installed

> >Which antivirus software is best for you will vary
> depending on your
> >computer systems, your security requirements and your
> personal preferences.
> >
> >Antivirus programs may be purchased from Internet web
> sites, from your local
> >computer store, and even from stores like Target and Wal-
> Mart. Antivirus
> >software can be found using the links below:
> >
> >www.symantec.com [Norton Antivirus]
> >www.grisoft.com [AVG Antivirus [including a free version]
> >www.f-prot.com/products [free DOS version]
> >www.f-secure.com [F-Secure]
> >www.trendmicro.com [Trend Micro]
> >www.wilders.org
> >www.download.com
> >www.tucows.com
> >
> >[Most of the antivirus products will also work on Windows
> Server products or
> >have a version for Windows Server.]
> >
> >There are also a number of web sites that will scan your
> computer for
> >viruses for free. However, using these web sites will do
> nothing to protect
> >you against future re-infection and damage to your
> computer files. Some of
> >these web sites include:
> >
> ><http://security2.norton.com> [Norton free one-time web-
> based scanner]
> ><http://housecall.antivirus.com> [Trend Micro free one-time
> web-based scanner]
> >
> >Just running an antivirus program is not enough. You
> should make sure that
> >your antivirus program can be configured to download
> updates every day [or
> >every week] automatically via the Internet, and open the
> program from time
> >to time to ensure that it is still receiving updates.
> >
> >Antivirus software is like prescription drugs or
> psychologists; the first
> >one you get might not work right for you. If one
> antivirus program fails to
> >install or causes your computer to perform slowly, you
> could contact the

Re: been hit by hacker, servudaemon installed

> > *manufacturer, or you could uninstall it and try another
> antivirus program.*
> >
> > *Note that you may need to set your antivirus program to
> ignore certain
> folders, such as the folder containing your firewall
> software. Failing to do
> so can cause speed problems or false alarms on your
> computer.*
> >
> > *You generally only want to install and run no more than
> one antivirus
> program on your computer at a time. Running two memory-
> resident, on-access
> antivirus programs simultaneously can cause false alarms
> or cause other
> problems.*
> >
> > *If you are running antivirus with the latest updates and
> are STILL having
> problems removing the virus, you should:*
> >
> > ** Note the name of the virus being reported by your
> antivirus program;
> * Visit the web site for your antivirus manufacturer and
> click on "Support,"
> so that you can:
> + Look up the virus name in the virus information
> database for info and
> follow any instructions found there;
> + Search the support web page for your antivirus; and/or
> + Post a question in the support group for your antivirus.*
> >
> > *For example, if you are using Norton Antivirus, you
> should visit the
> following web sites:*
> >
> > *www.sarc.com – NAV virus database
> www.sarc.com/techsupp – free NAV support discussion groups*
> >
> > *Be wary of any email ever that:*
> >
> > *Tells you to delete a file from your computer as the
> first or only way to
> remove a particular virus;
> * Tells you to forward the email to everyone you know;
> * Tells you that a particular virus cannot be stopped by
> antivirus.
> * Tells you that a particular virus has been confirmed by
> a large company or
> government entity, such as Microsoft, IBM, the Department*

> of *Defense, etc.*
> >
> > *Emails such as the ones described above are usually*
> > *hoaxes [even if the*
> > *warning email is from a friend that you trust]. Stop and*
> > *confirm or have*
> > *someone confirm the authenticity of any warning email*
> > *before forwarding it*
> > *to anyone. You can often confirm or deny the existence of*
> > *a particular virus*
> > *by searching for the virus name at an Internet search*
> > *engine or virus*
> > *manufacturer's web page, such as:*
> >
> > *www.google.com*
> > *www.sarc.com – Norton Antivirus*
> > *www.f-secure.com/virus-info – F-Secure*
> >
> > *TROJAN SCANNERS:*
> >
> > *It is also a good idea to consider using a Trojan scanner*
> > **in addition to**
> > *antivirus software. Trojans and hacker tools can cause*
> > *many of the same*
> > *symptoms that viruses and worms do, but antivirus*
> > *programs generally do not*
> > *detect all of the most common Trojans and hacker tools.*
> > *Some Trojan scanners*
> > *can be found by searching an Internet search engine or*
> > *your favorite*
> > *software web site, or by using the links below:*
> >
> > *www.pestpatrol.com [includes a free mini-scanner]*
> > *www.lockdowncorp.com*
> > *www.wilders.org*
> > *www.download.com*
> > *www.tucows.com*
> > *www.sunbelt-software.com*
> > *www.google.com/search?q=trojan-scanner*
> >
> > *When looking for Trojans, you should also consider using*
> > *a tool to look for*
> > *open ports, such as Vision or Fport from*
> > *www.foundstone.com/knowledge or*
> > *Pstools / Pslit from www.sysinternals.com*
> >
> > *For more extensive information about looking for Trojans,*
> > *backdoors and*
> > *other hacker tools, see the section in this FAQ*
> > *entitled "How can I tell if*
> > *I've been hacked?"*

microsoft.public.inetsrvr.iis.security: Re: been hit by hacker, servudaemon installed

> >
> >=====

> >
> >*Which firewall should I choose? Which firewall is the
> best?*

> >
> >*A: The answer to this question varies depending on your
> computer systems,
> your security requirements and your personal preferences.
> Below are some
> firewalls and other forms of firewall-like packet
> filtering:*

> >
> >*NO MATTER WHICH FIREWALL YOU CHOOSE...*
> >*No matter which firewall you choose, you should seriously
> consider
> downloading and installing 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.
> You can get this software at one of the links below:*

> >
> >www.mynetwatchman.com
> >www.dshield.org

> >
> >*Also, no matter which firewall you choose, the lists
> below of port numbers
> for common software services may be helpful when
> configuring your firewall
> or when trying to monitor the firewall logs for signs of
> intrusion:*

> >
> >www.iana.org/assignments/port-numbers
> >www.iisfaq.com/default.asp?View=P106

> >
> >
> >*FIREWALL SOFTWARE:*
> >www.sygate.com [*free for non-commercial use, also works
> like a sniffer*]
> >www.kerio.com [*free for non-commercial use*]
> >www.agnitum.com [*free for non-commercial use*]
> >www.zonealarm.com [*free for non-commercial use, also
> blocks pop-ups*]

Re: been hit by hacker, servudaemon installed

microsoft.public.inetsrvr.iis.security: Re: been hit by hacker, servudaemon installed

> >www.iss.net [*Black Ice*]
> >www.symantec.com [*Norton*]
> >www.webattack.com
> >www.download.com
> >www.tucows.com
> >[*Windows XP users can also consider using the ICF*
> >*firewall that comes with*
> >*XP, more info below*]
> >
> >*FIREWALL DEVICES [HOME / SOHO]:*
> >www.linksys.com [*starts around \$70 US*]
> >www.netgear.com [*starts around \$70 US*]
> ><http://search.ebay.com/search/search.dll?query=firewall>
> >[*prices on new and*
> >*used firewalls*]
> >
> >
> >
> >
> >
> >