

Re: win2000 has spyware, can I logon with console repair and delete files to

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2005-01/0285.html>

From: Bradley1234 (*someone_at_yahoo.com*)

Date: 01/17/05

Date: Mon, 17 Jan 2005 16:40:13 GMT

Aha, thanks Steven that helps. I ended up reformatting the drive yesterday, its a laptop with a super small 2.1G disk. It insists on making 2 drives, so I changed the fdisk setup, first by deleting all partitions, then loading msdos, tried to load win2000 but it wouldnt boot from the cd, (some cpu glitch) deleted the partitions again well anyway I changed them by 1, hoping that would throw off the file indexing mechanism

loaded SP4 which I thought enough to buy from Microsoft; then loaded Norton AV, did the live updates, 24Mb of stuff, and yanked the network cable as soon as that loaded

I had changed all security settings so that nobody can logon from the network, created guest account with long username and long pwd, must use ctrl/alt/del to logon, and whatever seemed right

never got the sasser worm this time.

But fell asleep doing the norton update as it took an hour, then it was beeping, found backdoor ? worm and ? beagle or ? worm blah blah

today did full scan, found 4 viruses and it says it cleaned them. it had a popup saying Windows updatez.exe was infected and kept generating it faster than I could click okay

so its sitting here behaving for a while, but its not on the network. Firewall? yes no doubt. I dont have one but they are very important. Im so out of the loop on how to manage win2000, I dont know if there is a free one, my dsl CD claimed to have one by MSN8 or ? but there is no setup window.

Well one thing for sure, viruses didnt just go away like a fad, they seem to be more prevalent than ever

"Steven L Umbach" <n9rou@nospam-comcast.net> wrote in message news:uejdREF\$EHA.2192@TK2MSFTNGP14.phx.gbl...

> *Well if it had that much malware on it and it was my computer, I would
> backup my needed data and do a fresh install to a formatted drive. If your*

microsoft.public.win2000.security: Re: win2000 has spyware, can I logon with console repair and delete files to

> computer has some backdoor root kits it could be very difficult to detect
> and remove them. If you do a reinstall be sure to take steps to prevent
> future infections. The main vulnerabilities are not using a properly
> configured firewall, not using a strong password for user accounts, not
> keeping current with virus definitions and not scanning ALL email
> attachments, using too loose security settings for IE, and not keeping
> current with critical updates at Windows Updates.
>
> Sounds like you are like me and like to check things out to try and figure
> out what is going on. If so, try downloading some free tools from
> SysInternals. In particular user Process Explorer, TCPView, and Autoruns.
PE

> can show the processes and map them to the owner executables and in
> properties of a process show what service it is if any. Be very suspicious
> of any process [that has a path to a file] that does not show a publisher
> name for the executable. Autoruns will show startup application/services
> from various places on your system and TCPView will show what executable
is

> using a port. --- Steve

>
> <http://www.sysinternals.com/ntw2k/freeware/procexp.shtml>

>
> "Bradley1234" <someone@yahoo.com> wrote in message
> news:jRAGd.957\$J6.834@trnddc02...
>> Hey thanks for that Steven. Im checking those websites now.

>>
>> The laptop was super duper infected. (is that the right way to say it?)

>> I

>> would start with dir a*.exe

>>

>> then let it show the exe names, and since Ive used DOS a lot over the
>> years

>> rather than spend time in a useful way, like at the beach, the odd named
>> ones I typed in and would delete spyware ones.

>>

>> But then I couldnt get into the registry manually, the regsvr32 /u
>> "filename" wouldnt work, in fact regsvr32 shows in the directory but

wont

>> execute at all

>>

>> I had downloaded the trendmicro virus scan thing you mentioned the night
>> it

>> happened. the download took almost an hour and it was so bad that one
>> mouse

>> click took at least 30 seconds to have any effect.

>>

>> doing cntrl/alt/del gets the control screen thing (windows2000 pro)
after

>> 5

>> seconds, but click on task manager would cause that box to disappear and

>> nothing would happen, well except the disk would be going full speed at

Re: win2000 has spyware, can I logon with console repair and delete files to

microsoft.public.win2000.security: Re: win2000 has spyware, can I logon with console repair and delete files to

> > *something.*
> >
> > *I was going to start it up and see what happened, but the most bad .exe*
> > *and*
> > *.dll files I found, and the fact I cannot unregister them, or even find*
> > *where the registry is at? (under a limited dos prompt) I put the*
original
> > *win2000 CD in there and am fixing it manually.*
> >
> > *It would report: hey dude, this isnt the original NTOSKRNL32 that I put*
in
> > *here originally, whats up with that? should I like, replace it or what?*
> > *and*
> > *I said do it*
> >
> > *then it said this file and that file and.... so I clicked all and it*
just
> > *finished updating and is rebooting win2000. lets see what it does*
now...
> >
> > *its booting very slowly, now there is an arrow against the blue screen,*
> > *now*
> > *its starting up, now an hourglass, applying security policy... I can*
check
> > *the football score and get some coffee while Im waiting... okay its*
asking
> > *for my old password to logon? okay, lets see, just an arrow against*
blue,
> > *super slow*
> >
> > *now it drew a box to load personal settings, took 1 second to draw the*
> > *box,*
> > *lines filled now the music, some disk activity, now its drawing the*
> > *desktop,*
> > *but why is it going so slow? its a p3 at 450... now arrow and*
hourglass,
> > *disk chugging*
> >
> > *clicks take a very long time, ctrl/alt/del and task manager? hmm nothing*
> > *is*
> > *happening, now its running trend micro virus scan...*
> >
> > *it only found 1 virus, 00004146.exe*
> >
> > *now lets look at add/remove programs*
> >
> > *BullsEye Network*
> > *Silicon Motion display driver*
> > *WebRebates (by TopRebates.com)*
> > *Winad Client*
> > *Windows SR 2.0*

Re: win2000 has spyware, can I logon with console repair and delete files to

microsoft.public.win2000.security: Re: win2000 has spyware, can I logon with console repair and delete files to

>>
>>
>> *"Steven L Umbach" <n9rou@nospam-comcast.net> wrote in message
>> news:uLBr35\$%23EHA.4072@TK2MSFTNGP10.phx.gbl...
>>> The best way is to use tools such as AdAware or the beta version of
>>> Microsoft's spyware remover AND to scan your computer with your
antivirus
>>> program being sure to update it's definition files first. The new MS
>> product
>>> has a "protect" mode to help prevent spyware installation. I have had
>> pretty
>>> good luck with it and it is available at the link below. Normally you
do
>> not
>>> need to reinstall the operating system unless your antivirus program
>>> finds
>>> significant problems with malware such as trojans, worms, and viruses
>>> indicating a highly compromised system that may also have undetectable
>> back
>>> doors such as root kits installed on it. --- Steve
>>>
>>> <http://www.microsoft.com/athome/security/spyware/software/default.msp>
>>> <http://mvps.org/winhelp2002/unwanted.htm> --- tips to help reduce
>> parasites
>>> [spyware, adware, hijacks]
>>>
>>> *"Bradley1234" <someone@yahoo.com> wrote in message
>>> news:58yGd.5570\$c%6.4380@trnddc03...
>>>> delete files to wipe out the spybot stuff?
>>>>
>>>> its my laptop, the first time I used it at a hotel on business, the
>>>> room
>>>> thing said to visit this website, click OK and YES to every question,
>> then
>>>> enjoy the internet.
>>>>
>>>> Guess what? It was saying yes to upload spyware and trojans into my
>>>> computer.
>>>>
>>>> I contacted the hotel and they played innocent saying we dont know,
its
>> a
>>>> secure and safe service, you must have visited "bad" sites or
>>>> something.
>>>> It was my first experience with spyware/spybot stuff, going to
>> add/remove
>>>> programs, it showed 3 or 4 which I tried to remove, it said please
>> answer
>>>> these questions and forward them to us: why do you want to uninstall?
>>> 1.
>>>> system too slow 2. dont like popups**

Re: win2000 has spyware, can I logon with console repair and delete files to

microsoft.public.win2000.security: Re: win2000 has spyware, can I logon with console repair and delete files to

> > > *etc...*
> > >
> > > *So my question is, now Im going to fix my laptop, used the win2000 CD*
> > > *to*
> > > *boot up and have a console prompt. Is there a common way you know*
> > > *about*
> > > *to*
> > > *delete the spyware bugs and fix the install? Do I have to delete all*
> > *and*
> > > *start over? Use the disk utility to write all zeros?*
> > >
> > > *thanks in advance*
> > >
> > >
> >>
> >>
> >
> >
>
>
>