

Re: viewing and deleting hacker created dirs

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2004-02/0003.html>

From: Robert Moir (*bofh_at_mvps.org*)

Date: 01/31/04

Date: Sat, 31 Jan 2004 18:52:35 -0000

I'd try installing a shell such as cygwin and use the 'ls' command from there to see what that finds.

I assume you've checked that the folder isn't simply marked as hidden or as a protected operating system object?

>From the looks of whats been going on, I'd also suggest a full rebuild of the problem machine, by the way.

--
--

Rob Moir, Microsoft MVP for servers & security

Website - <http://www.robertmoir.co.uk>

Virtual PC 2004 FAQ - <http://www.robertmoir.co.uk/win/VirtualPC2004FAQ.html>

Kazaa - Software update services for your Viruses and Spyware.

Agustin Chernitsky wrote:

> Hi guys,

>

> I found a service, which was created by a hacker, pointing to an exe file with this path:

> c:\WINNT\system32\vxd\poissonbulle\here\nbthlp.exe

>

> Now, I can browse up to c:\winnt\system32\vxd\, but if I do a "dir", I get nothing:

>

> <<<<

> Directory of C:\WINNT\system32\vxd

>

> 20/01/2004 08:12a <DIR> .

> 20/01/2004 08:12a <DIR> ..

> 0 File(s) 0 bytes

> 2 Dir(s) 37.210.169.344 bytes free

>>>>

>

> Still, if I do a cd \WINNT\system32\vxd\poissonbulle\here\ I can access that directory:

>

> <<<<

> C:\>cd \WINNT\system32\vxd\poissonbulle\here

> C:\WINNT\system32\vxd\poissonbulle\here>dir

>

> Directory of C:\WINNT\system32\vxd\poissonbulle\here

>

> 31/01/2004 01:37p <DIR> .

> 31/01/2004 01:37p <DIR> ..

Re: viewing and deleting hacker created dirs

microsoft.public.win2000.security: Re: viewing and deleting hacker created dirs

```
> 20/01/2004 08:48a <DIR> dmp
> 31/01/2004 01:37p 1.024 nbthlp.sys
> 31/01/2004 01:37p 49 ServUStartUpLog.txt
> 2 File(s) 1.073 bytes
> 3 Dir(s) 37.209.870.336 bytes free
>>>>
>
> The funny thing, is that doing a "cd .." I get:
>
> <<<<
> C:\WINNT\system32\vx\poissonbulle\here>cd ..
> The system cannot find the file specified.
>>>>
>
> As you can see, I can't see the .exe file also...
>
> My question is, is there a way I can see these kind of directories??
> I would like to see if there are more directories hidden in my system
> like this...
>
> I tried doing a dir /ad from C:\WINNT\system32\vx\, but nothing...
>
> I know I can remove the directory using rmdir
> \\.\c:\winnt\system32\vx /s
>
> By the way, since the directory is invalid, this service PID doesn't
> show in any process viewer or taskmanager (good trick).
>
> Thanks!
>
> Agustin.
```