

Re: Strange file in my root folder

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2005-02/0702.html>

From: Steven Burn (*somewhere_at_in-time.invalid*)

Date: 02/27/05

Date: Sun, 27 Feb 2005 17:01:26 -0000

Everything I've found suggests it is related in some way to VPN/SSL (no mention of it's legitimacy though)

--

Regards

Steven Burn

Ur I.T. Mate Group

www.it-mate.co.uk

Keeping it FREE!

"Daren" <pearcy@-removethis-gmail.com> wrote in message news:4221f92c\$0\$10947\$cc9e4d1f@news-text.

> Hello,

>

> I'm running windows 2k server. It's patched with all hotfixes, etc. Also
> has Norton AV and Kerio Personal Firewall.

>

> It is running a web site under IIS, so port 80 is open.

>

> I've discovered a file in the root of the c drive, called
> ur_tunnel_profile.log, at about 2mb in size. It was created at a time
> when no one was using the PC. Below are the first and last few lines of
> the file. Has anyone got an idea as to what this is? Has someone gained
> access to my PC?

>

> First few lines:-

```
> 17:31:08:031 (168) (768023843)
> 17:31:08:031 (168) ( 0) -----
> 17:31:08:046 (168) ( 16) open
> 17:31:08:046 (168) ( 0) -----
> 17:31:08:125 (2472) ( 137.67) win32_locking_callback enter
> 17:31:08:125 (2472) ( 0.05) win32_locking_callback enter
> 17:31:08:125 (2472) ( 0.02) win32_locking_callback enter
> 17:31:08:140 (2472) ( 17.67) win32_locking_callback enter
> 17:31:08:140 (2472) ( 0.06) win32_locking_callback enter
> 17:31:08:140 (2472) ( 1.62) win32_locking_callback enter
> 17:31:08:140 (2472) ( 0.05) win32_locking_callback enter
> 17:31:08:140 (2472) ( 0.70) win32_locking_callback enter
```

> .

> .

> .

> .

> Last few lines of file:-

```
> 17:45:50:078 (904) ( 0.03) begin statistics
> 17:45:50:078 (904) ( 0.09) end statistics
> 17:45:50:078 (904) ( 0.02) before select
> 17:45:50:250 (904) ( 167.27) select completed 1
> 17:45:50:250 (904) ( 0.06) << before read from remote side
> 17:45:50:250 (904) ( 0.12) << 17 bytes read
```

microsoft.public.win2000.security: Re: Strange file in my root folder

```
> 17:45:50:250 (904) ( 0.02) << before write to local side
> 17:45:50:250 (904) ( 0.28) << write completed
> 17:45:50:250 (904) ( 0.03) before select
> 17:45:50:343 (904) ( 107.95) select completed 1
> 17:45:50:343 (904) ( 0.06) >> before read from local side
> 17:45:50:406 (904) ( 56.58) >> -2 bytes read
> 17:45:50:453 (904) ( 50.33) before select
> 17:45:50:921 (904) ( 461.96) select completed 1
>
>
>
> Thanks,
>
> Daren
```