

microsoft.public.windowsxp.general: Re: Ok, so I'm a lazy moron – Explorer crashes at startup

Re: Ok, so I'm a lazy moron – Explorer crashes at startup

Source:

<http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.general/2004-05/27746.html>

From: kurttrail (*dontemailme_at_anywhereintheknownuniverse.org*)

Date: 05/27/04

Date: Thu, 27 May 2004 19:01:32 -0400

Steve Nielsen wrote:

> *kurttrail* wrote:

>

>> *Steve Nielsen* wrote:

>>

>>

>>> *Steve Nielsen* wrote:

>>>

>>>

>>>> *Kelly* wrote:

>>>>

>>>>

>>>>> *That is a whole lotta stuff loading/running there. With plenty*

>>>>> *.exe's. Will look more into it. Good luck in the meantime,*

>>>>> *Steve.*

>>>>>

>>>>

>>>> *Thanks Kelly. Yeah, most of it looks like the tablet PC goodies and*

>>>> *widgets to me.*

>>>>

>>>> *This just in...*

>>>>

>>>> *Now Spybot keeps finding these:*

>>>>

>>>> *DSO Exploit: Data source object exploit (Registry change, fixed)*

>>>>

>>>>

>>

>>

HKEY_USERS\S-1-5-21-2065366691-533095778-4141000609-500\Software\Microsoft\W

>> *indows\CurrentVersion\Internet*

>>

>>>> *Settings\Zones\0\1004!=W=3*

>>>>

Re: Ok, so I'm a lazy moron – Explorer crashes at startup

microsoft.public.windowsxp.general: Re: Ok, so I'm a lazy moron – Explorer crashes at startup

>>>> *Xer0x : Settings (Registry key, fixed)*
>>>> *HKEY_LOCAL_MACHINE\Software\xerox*
>>>>
>>>> *The 1st is an IE vulnerability, the 2nd is I believe actually there*
>>>> *due to a Xerox printer driver, not malicious but a false positive*
>>>> *due the name. I remove them anyhow but the puzzling thing is I have*
>>>> *Spybot fix them and they return. I'm almost thinking there might be*
>>>> *soemthing goofy with system restore and I'm gonna turn it off for a*
>>>> *while.*
>>>>
>>>> *I did post over in the tablet pc group, not as busy as here so no*
>>>> *replies yet.*
>>>>
>>>> *Thanks again*
>>>> *Steve*
>>>>
>>>>
>>>> *The Xer0x thing according to Symantec is a worm but none of the*
>>>> *files or registry entries associated with it exists on this system,*
>>>> *however it (and the DSO exploit) keeps re-appearing after every*
>>>> *reboot – even in Safe Mode and even after cleaning it with Spybot*
>>>> *S&D. I have spent quite a bit of time searching for information*
>>>> *about manually removing it but have found no other information. I'm*
>>>> *left to believe it is a new variant or some such and perhaps no one*
>>>> *knows yet how to deal with it.*
>>>>
>>>> *I got one reply so far in the tabletPC group saying it may be a bad*
>>>> *RAM module, but I'm dismissing that idea. I doubt flakey RAM would*
>>>> *present itself as a worm.*
>>>>
>>>> *Steve*
>>
>>
>>
>>
>>
<http://securityresponse.symantec.com/avcenter/venc/data/w32.hllw.loxar.html>
>>
>> http://vil.nai.com/vil/content/v_100752.htm#RemovalInstructions
>>
>> *I don't know, but I'd assume XP Tablet has safe mode. Boot into*
>> *that as the Administrator, clear out all the System Restore backups,*
>> *then disable System Restore. Then clean up the registry & search*
>> *for any of the Xer0x files.*
>>
>> *And don't forget to scare the living sh*t out of the Luser for his*
>> *filing sharing habits.*
>>
>> *<asside: This is my second attempt. I forgot to put the "*" in*
>> *"sh*t">*
>>
>

Re: Ok, so I'm a lazy moron – Explorer crashes at startup

microsoft.public.windowsxp.general: Re: Ok, so I'm a lazy moron – Explorer crashes at startup

> *ROFLMAO!*

>

> *Yeah, it has Safe Mode and I already did all this stuff except I*

> *thought turning off system restore automatically removes all restore*

> *points, it still persists.*

>

> *Steve*

Have you tried CWShedder?

--

Peace!

Kurt

Self-anointed Moderator

microsoft.public.windowsxp.gonorrhea

<http://microscum.com>

"Trustworthy Computing" is only another example of an Oxymoron!

"Produkt-Aktivierung macht frei!"