

## Re: Ilomo trojan-regscan- how do I zap this thing?

---

*Source:*

<http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.general/2008-01/msg00231.html>

---

- *From:* "Pegasus \ (MVP)" <I.can@xxxxxxxxxxx>
  - *Date:* Wed, 16 Jan 2008 17:59:38 +0100
- 

"Danny Sanders" <DSanders@xxxxxxxxxxxxxxxx> wrote in message  
<news:OvQyaAGWIHA.2268@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

When you get a virus there is really no way to know if you have *\*really\** gotten rid of it or not. What happens if you jump through all the hoops and rings you find here and there about getting rid of this Trojan and you think you have everything cleaned up and working nicely, and the first time you open notepad, which is really his file he renamed and put there just for this purpose, the Trojan gets installed again and opens the door to your server to him again?

The point is you can go through and do everything you see on the 'net about getting rid of the Trojan but there is just no way to be sure there are no renamed Windows files on that server that will open it up as soon as you think you are done. The *\*only\** way to be sure is to format – reinstall and restore from a backup before the Trojan hit. Sure it's a lot of work but it's a lot of work to jump through all the hoops and edit the registry only to find that the is back after rebooting the server. Cut out the extra work and format – reinstall and restore from a backup before the Trojan hit.

Use the time you would have spent trying to get rid of the thing to secure the server. Install virus software make sure the server is regularly updated, lock down the firewall in front of this server and make sure only the necessary services are exposed to the Internet and make sure to keep on top of patching those exposed services.

Recover quickly and spend your time making sure it doesn't happen again.

hth  
DDS

"Chopper" <HeyJoe@xxxxxxxxxxx> wrote in message  
[news:478e2ab6\\$0\\$18416\\$4c368faf@xxxxxxxxxxxxxxxxxxxxxxxx](news:478e2ab6$0$18416$4c368faf@xxxxxxxxxxxxxxxxxxxxxxxx)

CA anti-spyware scan detects Ilomo Trojan in regscan.exe and tries to

Re: Ilomo trojan-regscan- how do I zap this thing?

quarantine unsuccessfully. If I turn off auto quarantine I get a buffer over-run. When I re-scan right away, I get the same results. I can't find regscan.exe on my hard drive, either searching manually or with search function. I have everything turned on to show hidden and system files. CA anti-virus shows no infection.

I'm running win2k, Sp4, update rollup 1 v2. When I boot into safe mode it takes a long, long time, and any program I try to run starts very slowly. Task manager doesn't show anything out of the ordinary running, either in normal boot or safe mode. Could the extremely slow boot into safe mode be related to this trojan?

Latest scan log:

1/14/2008-6:40:42 PM , Detected , Ilomo , Trojan , File

"C:\WINNT\system32\regscan.exe" , -1

1/14/2008-6:40:42 PM , Detected , Ilomo , Trojan , Key "hkey\_user

\S-1-5-21-842925246-115176313-725345543-500\Software\Microsoft\Windows\CurrentVersion\Run" value "Regscan" , -1

1/14/2008-6:41:28 PM , Quarantined , Ilomo , Trojan , File

"C:\WINNT\system32\regscan.exe" , -1

I also have temp files in temp directories-local disk\Documents and Settings\Administrator\Local Settings\Temp- with names like ~DF11F8.tmp that

don't delete when I clear cache and when I try to manually delete I get message saying they are in use and new temp files immediately appear with similar names. Older temp files can be deleted, but not the new ones that are spawned. Is this normal or could it be related to this trojan?

My desktop icons randomly relocate on boot up, and I noticed file named index.dat in - local disk\Documents and Settings\Administrator\Local Settings\History\history.IE5 and other locations that don't delete when I clear cache. Also find desktop.ini files buried in subfolders under temporary internet files folders. Could these be related to trojan?

I have googled this problem and gone to quite a few sites including CA, McAfee, Eset, Trend Micro and others and can't find an answer how to eliminate this pest.

Reading between the lines of what I have found, I think I need to edit the registry and delete the hkey\_user data, but I'm not real familiar with how to do safely. I believe I need to delete regscan.exe also, but to re-iterate, I can't find it on disk.

Any advice would be appreciated, with enough detail for someone not real familiar with editing the registry.

Re: Ilomo trojan–regscan– how do I zap this thing?

Well said. There is another angle to it too: Unless the virus is extremely well documented, the OP will never know what damage it did. Some of the damage may not become apparent until much later. Many virus writers derive pleasure from corrupting a file here, a registry entry there, often randomly.