

## Re: Trojan.Dropper: tempms.exe

---

*Source:* <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2007-01/msg00063.html>

---

- *From:* "chuck" <[chuck@xxxxxxxxxxxxxxxx](mailto:chuck@xxxxxxxxxxxxxxxx)>
  - *Date:* Tue, 9 Jan 2007 01:28:44 -0800
- 

Thanks for your help. I have run the scan in safe mode with Symantec AV. Nothing found.

I then reboot. Install and scan with SpyBot. There are several registry entries found and destroyed. But the winxx.exe still got replicated like crazy in my "\\Documents and Settings\\user name>\local settings\temp folder. I then installed Node32. I scanned the hard disk with Nod32. No threat was found.

Now I keep having a dialog popping up from Nod32.

<http://www.ucdq.com/k.exe>

Probably unkonown NewHeur\_PE virus

I chose to terminate it. But the dialog keeps coming up. I keeps killing it.

Have you heard of this virus?

I checked Google for [www.ucdq.com](http://www.ucdq.com). All the articles are in Chinese. It looks like a Asian virus.

"Panda\_man" <[Pandaman@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:Pandaman@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)> wrote in message [news:B186D110-52F9-4CEE-87DE-8A4FB9BC4DE3@xxxxxxxxxxxxxxxxxxxx](mailto:news:B186D110-52F9-4CEE-87DE-8A4FB9BC4DE3@xxxxxxxxxxxxxxxxxxxx)

"chuck" wrote:

My Symantec Antivirus always warns me of a Trojan.Dropper in c:\Windows\System32\tempms.exe. But I could not find that file in that folder.

Does anyone know what went wrong? Is it related to the replicating winxx.exe files in my temp folder as I post in a different post?

Re: Trojan.Dropper: tempms.exe

Hello .

Boot your computer in Safe Mode . Disable System Restore and perform full scan with Symantec AV .

After you reboot , perform the Malware removal instructions here  
<http://pandaman.my.contact.bg>

Let us know what happened :-)

--

Panda\_man  
Silver level Contributor