

Strange malicious script/spyware dropper/virus DOService

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2003-12/0645.html>

From: Lindsay (*anonymous_at_discussions.microsoft.com*)

Date: 12/09/03

Date: Tue, 9 Dec 2003 01:21:05 -0800

My boyfriend had a little *ahem* accident the other day in which he clicked "yes" accidentally to a box that popped up on a website.

Now his computer is plagued with problems. He's running Windows XP, unsure what service pack because I am not there to look at his comp, however since clicking this link the following things have happened:

1) 9-10 svchost.exe tasks running, using 99-100% CPU time, making it unable to do ANYTHING without being in safemode.

-I had him do a search for the program and found two instances:

C:\Windows\System32\svchost.exe *the valid one*

C:\Windows\svchost.exe *the questionable one*

-Upon deleting the one in the "Windows" folder, he is now able to restart in normal Windows mode without having the CPU time. He's back down to approx. 4-5 processes running now. I'm assuming that was the culprit/virus.

2) Since clicking on this link, numerous spyware programs have been dropped on his computer, ie) ones from n-Case, ezSearchBar, istsvc.exe ??, and more. IE homepage address has been changed to match the ez-search.net site. This too was caused by this malicious script, and here's the kicker:

3) To uninstall n-Case and the other spywares, you have to access the internet. My boyfriend is on a LAN with his family, running a firewall on their server, and he has antivirus protection, which baffles me as to why it didn't catch this. He has updated definitions.

Well, this little SOB virus has also figured out how to

microsoft.public.security.virus: Strange malicious script/spyware dropper/virus DOService

disable internet access. The network connections say that it is connected to the network, however when he opens internet explorer NOTHING will connect. I know that this is not related to the svchost.exe file, because the one that exists is supposed to be where it is.

The Repair option for the network does no good, it simply again says "Local Area Connection : connection speed" as if he's connected to the network. He's tried disabling it and re-enabling it, to no avail.

Is it possible that this virus has screwed with his internet settings as well? I know it's possible.

I've found little to nothing in reference to a virus with C:\Windows\svchost.exe, and even less relating to the spyware dropping.

We've also both had problems with bitTorrent lately, as have a few friends. Since installing bitTorrent from the real programmer's site, we've had issues with system instability, crashing, and freezing. I have been the least infected, however I am also the one running a firewall with tight options and backed by lord knows how many college firewalls. Several friends have had computers crashing using this program. Is it possible that the virus and spyware dropper could be related to bitTorrent instead of the website he visited? I mean, could someone have figured out how to exploit something with the svchost.exe file through bitTorrent, sort of how the whole RPC viruses were doing through the internet by sending packets to cause buffer overflows?

Has anyone heard of any of these things and can lead me to an answer? He really doesn't want to reformat, and since we've got the computer up and running again I feel that if the internet problem could be solved, we could not only get rid of that nasty spyware but also get an updated firewall for him and see what the virus scanner has to say.

Thanks to all for suffering through this, I know it was a long post, and any help is appreciated,

~Lindsay