

Re: Help me,my computer maybe at risk with some trojan.

# Re: Help me,my computer maybe at risk with some trojan.

---

*Source:* <http://www.derkeiler.com/Newsgroups/comp.security.misc/2008-04/msg00023.html>

---

- *From:* Olicaca <jolibama@xxxxxxxxxx>
  - *Date:* Thu, 10 Apr 2008 07:00:28 -0700 (PDT)
- 

On Apr 10, 8:10 pm, "Sebastian G." <se...@xxxxxxxxxx> wrote:

Olicaca wrote:

Why don't teach me how to check if a trojan stay on ur computer instead of reasoning

Simply said, since I make sure there're no point to hook into, any malicious software would have to appear as a separate process in the process list. That's trivial to check.

> arguing, about the reason of bug on the PC..?

Well, that's the reason why I suggest to create an disk image of the compromised system. Later on you may start analyzing what malware it is and which security hole was exploited. It's pretty unlikely that it wasn't a configuration or random problem, which is unlikely to occur again. You don't have to the put the system online either.

> You really think antivirus can check out all trojan huh?

No. Analysis are normally conducted with serious tools.

> Do you hear that if you have trojan on source setup than it quite

pass anti-shitwares check??

Well, that's pretty trivial.

I'm acquainted with some friend and he declares that,if he write a trojan then no antivirus can detect, because his is not destroy anything and...

Re: Help me,my computer maybe at risk with some trojan.

Well, although this is generally possible, the argument is bogus. The real argument is that one can create malware that modifies itself in a way such that no L0, L1 or L2 pattern signature could match it in every fashion, and not even behaviour analysis would conclude anything.

> Virus and worm is easy to detect but trojan is not,specially it

is the economic war.

They're only detectable by their defined behaviour, that is a virus does modify other executables, and a worm modifies the behaviour of server processes.

> You say manything and about bandwidth but i need u teach how to detect

trojan,bandwidth is no problem.

What I said is that bandwidth is a valueable resource that is definitely in the interest of the attacker.

> Could you help?

How many more times do I have to ask you if you have flattened and rebuild the system? Bring it back to a well-defined state first, since this is the only reliable way to recover from a compromise.

> Ah,if you want teach me

then please use English in the simple grammar,hornestly i'm idiotic in English maybe and i must try so much to understand.It is real(coz my country not use English and not join with the World soon).

"coz" is obviously not an English word.

---

Ok,now we begin have the common voice.I reinstall OS and creat backup image but nothing resolved.Because right here,most of us use unofficial CD to install OS.I just want check my resource.So let help me check hooked module and handle...,really i don't know how to check it,and the open port too.I want get some files to send out to analysis.If my CD is dirty then certainly i will buy one but first must bring everything to light.Could u help?Ok,and notice that i'm a home user,not a networking man,so i was wrong when didnt read the "about this group".Maybe you not a security agent to treat malware :

Re: Help me,my computer maybe at risk with some trojan.

Re: Help me,my computer maybe at risk with some trojan.

((.Maybe i will go to bitdefenden forum better use google group.Bye  
bye.

"Coz" = because and "brb"=be right back ja.I'm just using familiar  
chatting English,not know formal language,forgive me.

.