

reply

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2003-11/2349.html>

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

Date: 11/26/03

Date: Tue, 25 Nov 2003 17:17:22 -0800

>-----Original Message-----

>There is a "trojan horse" program in my PC that refuses to
>be removed. I have tried Ad-Aware, Spy Bots and also
>tried deleting it from the msconfig Startup tool system,
>and searched for it in the registry, but I am unable to
>remove it. I unchecked it in the msconfig Start up
>program, but it reappears again with a checked box on a
>new line in the list. It listed name is: 2N7NDTN44L@@AN,
>and a command name in the windows system that changes each
>time it returns in the Startup list, example
>C:\Windows\system\OqxNq.exe. When I tried the Search
>function, neither the listed name or command line name
>produced any results. It constantly generates web page ads
>on my pc. Is there any other method I can use to remove
>it?. I suspect it was attached to a free copy of a
>downloaded Grisoft AVG Anti Virus software. I have a
>Presario Intel 4,1.7GHZ PC with 256RAM and Win ME.
>
>Peace through understanding,
>
>
>
>

Reply:

The reason that it keeps replicating itself is that there is a mother file that is set to do such, from another location. You need to delete the mother file or the replicating won't stop. It is probably hidden, as well as the replicated files, this is why WinME won't pick them up in the search. I have a couple of suggestions:
First, ME comes with a registry backup application, try restoring an old registry backup, this may remove all

registry keys that are generated by the trojan.

If the replicated files keep appearing in the
C:\windows\system\ folder, try locking access to this
folder temporarily by using attrib.exe:

In DOS (you may have to restart into DOS to lock this
folder since it is in use), type:

```
cd\  
attrib +r c:\windows\system\
```

this can be undone later in DOS by typing:

```
cd\  
attrib -r c:\windows\system\
```

(write down the undo command line, if Windows does not