What's this, a Windows virus running on my Mandriva?

Leo Kavanagh 6 June 2008

A few days ago as I was searching for new legal downloads on Bit Torrent, I saw a Windows jig-saw puzzle and thought about a certain Linux member, who I know likes these games.

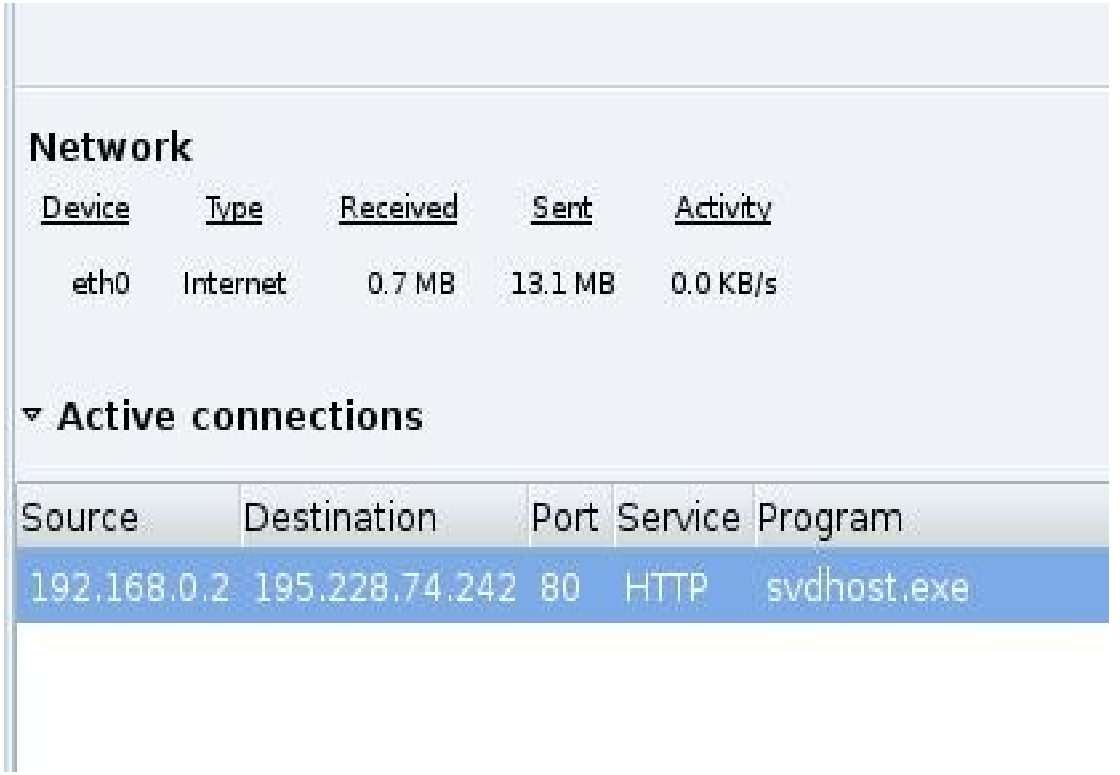
I downloaded it, presuming of course that it was a trial version and thought to myself "I wonder if it will run on Linux under wine" so I clicked on the xxxxxxxx.exe file and it appeared to install with no problems.

It depended on Adobe Flash Player which was installed on my system but when I tried to run the game I got an error message "Unable to open Adobe Flash Player". No amount of playing around could get it to run as designed but I could open the individual ".swf" files (shock wave flash) and play that segment of the game.

Later I wanted to search on Google so I opened Firefox, clicked the Google Bookmark and the Google page started to open and then locked. Most unusual. Looked at my Router and the LED's were blinking at full speed. Curious so I clicked on the button "Active Connections" in my gui firewall - Firestarter and much to my surprise I saw the active connection. I hit the router switch to quickly turn it off and took a Screenshot.

See the next page for the culprit:

What a surprise to see a Windows System File on my Linux partition had hijacked Port 80 and was uploading data. "Activity" shown on Firestarter is zero as by this time I had switched off my Router.



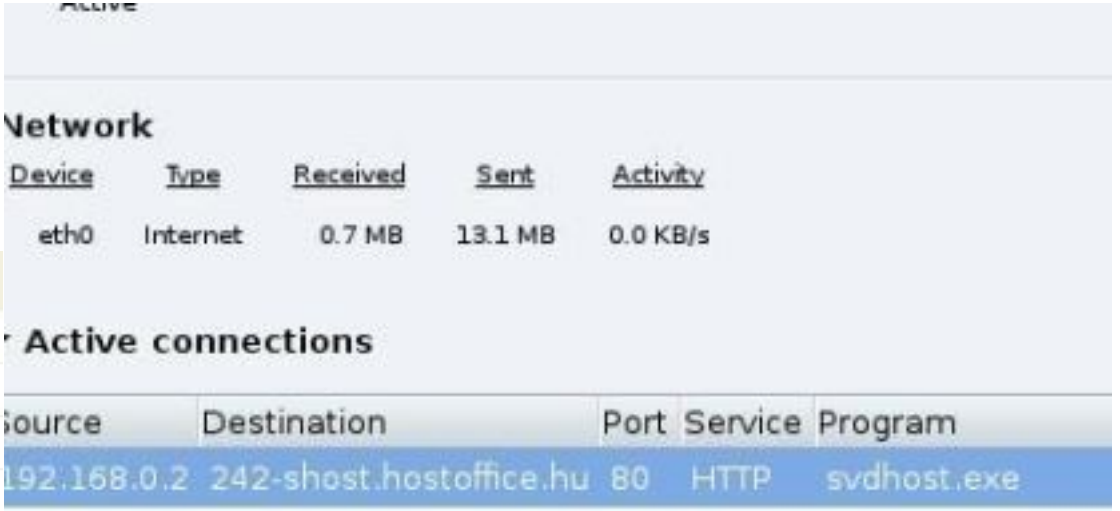
Wine is a great piece of Software and I had been running the Windows IrfanView graphic program with great success, but a Virus!

A virus indeed as a quick Google search showed:
svdhost.exe - Dangerous
Svdhost.exe is W97M.Mupps. W97M.Mupps is a Trojan horse that opens a back door to a remote location on the compromised computer.

The client component runs on the attacker's computer, and connects to the server component on the victim's machine remotely.

A quick check on Firestarter shows the URL of the connection, see next page:

Firestarter can also show the URL of most IP address and it shows that my data has been sent to a country that shields these malware writers.



Network

Device	Type	Received	Sent	Activity
eth0	Internet	0.7 MB	13.1 MB	0.0 KB/s

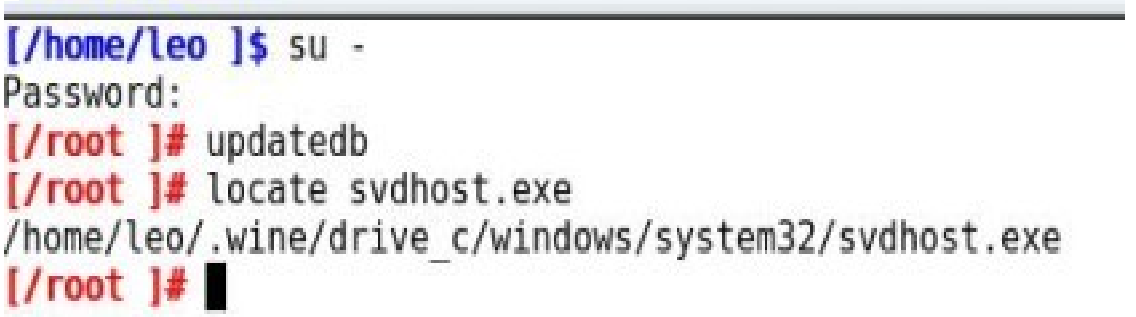
Active connections

Source	Destination	Port	Service	Program
192.168.0.2	242-shost.hostoffice.hu	80	HTTP	svdhost.exe

195.228.74.242 - Geo Information

IP address	195.228.74.242
Host	242-shost.hostoffice.hu
Location	HU, Hungary
City	Budapest, 05 -
Organization	HostOffice Informatikai Szolgaltato es Kereskedelm
ISP	Hungarian Telecom MATAV

The virus does indeed reside on my Linux home partition and a quick search of my Windows XP shows that it is non-existant, only the Windows system file svchost.exe is there.



```
[/home/leo ]$ su -
Password:
[/root ]# updatedb
[/root ]# locate svdhost.exe
/home/leo/.wine/drive_c/windows/system32/svdhost.exe
[/root ]#
```

When wine is installing a Windows program it creates an environment that makes the program think it is running on Windows. It creates a C:\ and all the necessary system files underneath this, all in the home partition on Linux. You don't even need Windows installed on the computer.

A make believe Registry is also created and this is where most virus create an entry to make sure they run on every boot.

http://vil.nai.com/vil/content/v_139508.htm shows:
The following Registry entry is modified, so the Trojan runs on startup:

* Hkey_Local_Machine\Software\Microsoft\Windows\CurrentVersion\Run
  "Login" Data: C:\Windows\svdhost.exe

When I look in my make believe Registry: /home/leo/.wine/system.reg
I see these two entries, almost the same as in the Windows registry:

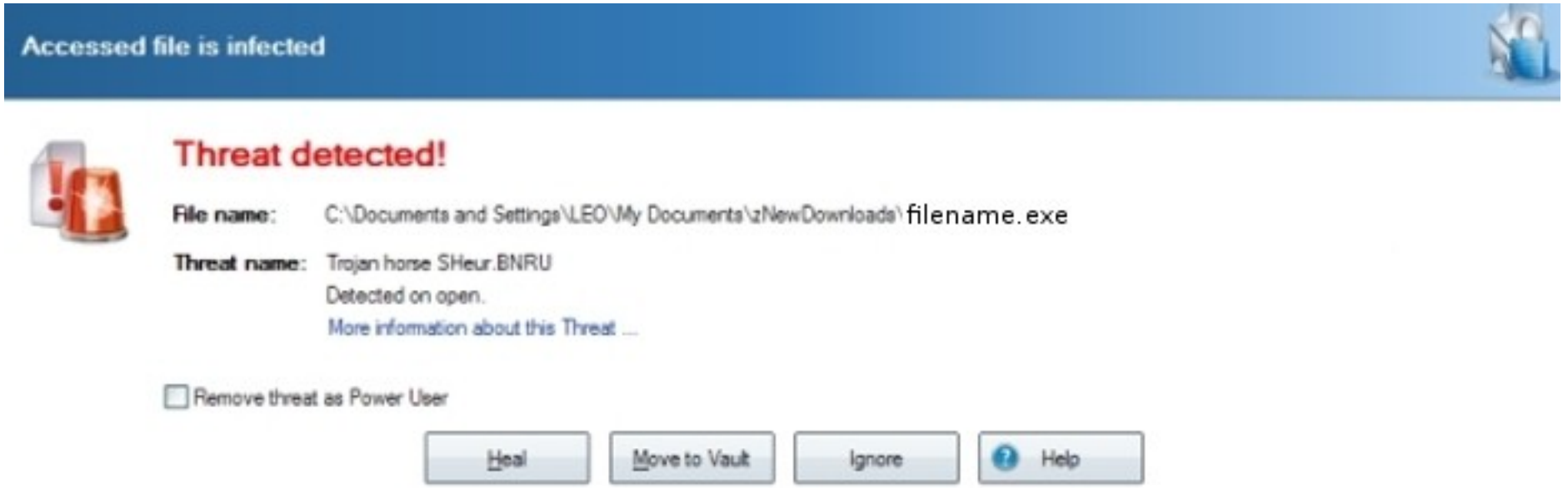
[Software\\Microsoft\\Windows\\CurrentVersion\\Run] 1212351995
"Windows Sound"="svdhost.exe"

[Software\\Microsoft\\Windows\\CurrentVersion\\RunServices] 1212351995
"Windows Sound"="svdhost.exe"

Perhaps in hindsight I should have scanned the .exe file before I installed it on my Linux partition. We all know that a virus running as user cannot alter any of our system files but as you see here, when you give a virus permission to run on our home partition it can do anything to our user files and also scan our home partition and hijack Port 80 (which we can't close) and send our personal data to another country.

There is plenty of information on the web about this malware and when I scanned the file with AVG anti-virus on Windows, the virus was immediately detected.

A quick scan of the file with AVG anti-virus shows the problem



The problem is easily solved in Linux, just delete the hidden folder /home/leo/.wine/ and all the Windows rubbish is totally removed. But just to be safe and remove any files that may have been written to my /home partition, I used a 2 day old home partition backup and restored my partition to it's virus free status.

Even though we have a very secure Operating System, we should not give a Windows virus permission to do what it wants with the help of "WINE" on our home partition.

END