

strange safe.w2kserver1.com connections, spyware?

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2006-02/msg00129.html>

- *From:* "none" <mikem891@xxxxxxxxxxxxx>
 - *Date:* 27 Feb 2006 16:29:48 -0800
-

Hi,

Last week I noticed very strange reports from my firewall on my win2k system and found out that every running applications where trying to contact these 2 servers (very often):

safe.w2kserver1.com 216.55.181.80
safe.w2kserver2.com 216.55.181.96

Doing a search in google I didn't find anything except these 3 german discussions:

http://www.nickles.de/static_cache/538027763.html

http://www.nickles.de/static_cache/538032330.html

<http://www.wcm.at/forum/showthread.php?threadid=186064>

And I don't speak german :-> I translated it but they do not seem to know what's it really does.

Scanning my computer with spybot s&d, adaware and avg a/v didn't detect any problems.

So I decided to try to find it using Process Explorer and found a strange file attached to every processes:

file: E:\WINNT\System32\slpube03.dll

size: 139,264 bytes

MD5 : c836b88308984f5fe7aaab488ffa1156

Internal Info:

File version: 5, 1, 2600, 0

Company name:

Internal name: Shell Publishing

Comments:

Legal copyright: Copyright 2000

Legal trademarks:

Original filename: slpube03.dll

Product name: Shell Publishing Module

Product version: 5, 1, 2600, 0

File description: Shell Publishing Extension Module

Private build:

Special build:

strange safe.w2kserver1.com connections, spyware?

Searching in the file with an HEX editor I found the strings:
"safe.w2kserver1.com" and "safe.w2kserver2.com"

So I thought that this was the file I was searching for so I have
unregistered it from the COM dll server and rebooted

And everything was back to normal!

I also found this registry values in the registry:

[HKEY_LOCAL_MACHINE\SOFTWARE\SourceSafe]

[HKEY_LOCAL_MACHINE\SOFTWARE\SourceSafe\1.0]

[HKEY_LOCAL_MACHINE\SOFTWARE\SourceSafe\1.0\ Cache]
"W2kIP1"="<http://safe.w2kserver1.com/>
"W2kIP2"="<http://safe.w2kserver2.com/>

Then I tried to desinstall and reinstall every programs I've downloaded
the same day and found out that the program I suspect to install it is:

DivX DVD Ripper 1.6 (or 1.5) from Video Voodoo
I've download it from <http://www.openwares.org/>
the file can be found there:
<http://www.openwares.org/file.php?&Itemid=39>

If you uninstall it, it open a IE windows to the
<http://www.openwares.org/> site. So maybe the spyware is installed by
www.openwares.org I really don't know.

I said I suspect this file to have installed the software because I
didn't give it any access to any 216.55.181.XXX addresses for security,
so It was not able to reinstall the dll file and I can't be sure of it.
But during the installation the install programs tries to contact the
following IPs:

www.mediaplace.tv [216.55.181.78]

www.dnscaching.net [216.55.181.75]

Since they are on the same network as w2kserverX, I'm pretty sure they
are related.

Zilla CD-DVD Rip N' Burn from the same site (www.openwares.org) seems
to also make these connections

Another thing that I saw while doing the installation is that a process
called:

file: [SpreadFirefox.exe](#)

it is launched and is found in the \document and
settings\administrator\local settings\temp\ directory

When I first saw the safe.w2kserverX.com connection, just before I saw

strange safe.w2kserver1.com connections, spyware?

strange safe.w2kserver1.com connections, spyware?

that a strange process called ~nsisload.exe was running but I don't know if they are related.

From the string tables in the slpube03.dll file, it's seems to read or

write the following to registry keys:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Shell Extensions\Approved

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers
But I inspected these keys and found nothing suspicious.

If for some reasons DivX DVD Ripper, www.openwares.org are not the one responsible for the spyware install, I'm really sorry. I do not want to make bad publicity for them if they are not related to this.

So to remove do the following

1 – goto START/RUN and type:

regsvr32 /u C:\WINNT\System32\slpube03.dll

2 – delete the file C:\WINNT\System32\slpube03.dll (you may need to reboot)

3 – start regedit (START/RUN/ type regedit)

delete the following key

HKEY_LOCAL_MACHINE\SOFTWARE\SourceSafe

4 – reboot

Now the network connections should be over.

Is anyone has some information about this case? Is it a spyware? Please post any infos regarding this. I may have forget something and maybe something is still left on the system.

I have contacted AVG and spybot search & destroy regarding this case and I didn't received any reply yet. And their scanners do not detect it yet.

Thanks

.