

Re: NORTON Firewall doesn't detect TROJAN, !!WARNING TROJAN ATTACHED!!

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2002-12/1863.html>

From: Hunter Watson (djgka876@keocm.net)

Date: 12/19/02

From: Hunter Watson <djgka876@keocm.net>

Date: Thu, 19 Dec 2002 05:24:13 GMT

On Tue, 17 Dec 2002 06:53:25 GMT, "Pear Annoyed"
<computeruser@127.0.0.1> wrote:

*>If this is not a joke (Amy_orgasm? if true, couldn't you at least change
>the name?),*

No, this is not a joke. I am not ashamed to admit I was trying to look at some porn. If the attachment would have made it in the first post you would have seen the name of the file anyway. I wasn't going to alter anything in case someone that knew there shit could have helped me. Your suggestion to rename the file seems prudish.

You obviously didn't read my full post or didn't comprehend it because of your reply below.

*> I think Realplayer was just trying to download a new codec to
>run your porn movie, the spooler probably was trying to give information
>so Realplayer would know exactly what to download.*

First>> the logs from the 1st post>>>

>>Alert 12/16/2002 17:49:07

>>Remote address,service is (wwp.mirabilis.com(205.188.248.25),http(80))

>>Process name is "C:\WINDOWS\MS SPOOL32.EXE"

>>Alert 12/16/2002 17:49:13

>>Remote address is (messenger.hotmail.com(207.46.104.20),msnp1863

>>Process name is "C:\WINDOWS\MS SPOOL32.EXE"

What does "wwp.mirabilis.com" (an IRC Server) have to do with codecs from "real.com". Or what does "messenger.hotmail.com" have to do with codec downloads from "real.com".

Second>>(from the 1st post)

>>The first thing I did after re booting was check "view statistics" with NIS.

comp.security.firewalls: Re: NORTON Firewall doesn't detect TROJAN, !!WARNING TROJAN ATTACHED!!

>>Normally the only connection open after re booting is "symproxysvc.exe".
>>But there were 2 connections opened, "ms spool32.exe" and "symproxysvc.exe".
I have D/L codecs from "real.com" before and realplayer never started
MS SPOOL32.EXE. My 1st post also said " MS SPOOL32.EXE and 2 other
files were created when I clicked on the .ram file".

Third>>(from the 1st post)

>>I opened "first_3sum.wri" again in MS Wordpad and highlighted "Amy_orgasm.ram"
>>and selected "edit package". The appearance window said " Amy_orgasm.ram"
>>but the content window said "copy of dynu.exe".
Doesn't an executable file packaged and renamed as a realmedia file
seem suspicious to you?

Fourth>>(from the 1st post)

>>"MS SPOOL32.dat" contains a list of .exe files I think "ms spool32.exe" is trying to shutdown.
>>A few samples from "MS SPOOL32.dat">>>>
>>(NAVAPW32.EXE, IAMAPP.EXE, ZONEALARM.EXE, VSHWIN32.EXE, REGEDIT.EXE,
>>DRWATSON.EXE, SYSEDIT.EXE, NETSTAT.EXE, SCONFIG.EXE, GUARD.EXE,
>>UPDATE.EXE, AUTOUPDATE.EXE, CLEANER.EXE, UPDATE.EXE, ANTI-TROJAN.EXE,
>>WATCHDOG.EXE, BLACKICE.EXE, LUCOMSERVER.EXE, TASKMGR.EXE,
>>GUARDDOG.EXE, ZONEALARM.EXE).

>>"MS SPOOL32k.dat" contained by date and time all the
>>programs that were opened and the keystrokes I made in those programs.
>>I could see my sign on password, my social security number and
>>password for my 401K web site. I'm lucky I blocked "ms spool32.exe"
>>from connecting to the internet.

All of the above sounds like backdoor trojans I have been reading
about. Since the first post I have opened "ms spool32.exe" in notepad.
There were lots of code which was garbage to me cause I don't know
much about that shit. But I do see references to the 2 .dat files
listed above. Also a reference to "Keylogger.dll" and
"GetKeyboardType". I think this is a trojan and NIS failed me on this
one. I am trying to resolve it with Symantec but their support sucks.
It seems no one there has read my comments and only ran the file
through NAV. Or it is all automated and no person has reviewed my
comments. I am going to paste my original post below in case you have
already deleted it. Please check it out again.

Thanks for your help.

ORIGINAL POST BELOW>>

WARNING!!! ATTACHED FILE IS INFECTED WITH A TROJAN.
DON'T OPEN UNLESS YOU KNOW WHAT YOUR DOING.

Below is my reply to Symantec were they said there was no problem with
the trojan I sent to them for inspection. Maybe I'm wrong. Please
read my post and tell me what you think. For you guys that know your
stuff please check out the attached infected file and please give me
some advise on how to completely remove the infection.

Thanks

Re: NORTON Firewall doesn't detect TROJAN, !!WARNING TROJAN ATTACHED!!

comp.security.firewalls: Re: NORTON Firewall doesn't detect TROJAN, !!WARNING TROJAN ATTACHED!!

Below is my reply to Symantec>>>>>>>>

This is a response to Tracking #2291036 which is pasted at the end of this note.

My OS is Windows ME. I am using Norton Internet Security(NIS)2002.

If you read below and repeat the steps I outline below you will see that the file I'm sending is a trojan and NIS 2002 did not find this trojan that infected my computer. Please open " view statistics" in NIS and record the executables running in the "network connections" window. Then open "first_3sum.wri" with MicroSoft(MS)Wordpad. Then double click on the icon for "Amy_orgasm.ram". and you will see "ms spool32.exe" has a port open in "network connections".

I Received an e-mail with a file called "pictures.zip" attached. Inside the .zip file was a file called "first_3sum.wri". I opened the .wri file with MS Wordpad. There are 3 objects packaged inside the file "first_3sum.wri". The first 2 objects were jpeg files which opened OK when I double clicked on them. The third object was a video file called "Amy_orgasm.ram". When I double clicked on the .ram file the computer did nothing for 10 seconds then "Realplayer" came up and said there was a problem with the file. I went online to Real.com and NIS was warning me that a file called "ms spool32.exe" was trying to connect to the internet. The log entries from NIS 2002 are pasted here>>>>

Alert 12/16/2002 17:49:07 IP Filter This one time, the user has chosen to "block" communications. Details:
Outbound TCP connection
Remote address,service is (wwp.mirabilis.com(205.188.248.25),http(80))
Process name is "C:\WINDOWS\MS SPOOL32.EXE"

Alert 12/16/2002 17:49:13 IP Filter This one time, the user has chosen to "block" communications. Details:
Outbound TCP connection
Remote address,service is
(messenger.hotmail.com(207.46.104.20),msnp(1863))
Process name is "C:\WINDOWS\MS SPOOL32.EXE"

This type of alert only happens after I instal new software that can access the internet. I haven't installed any new software in months.

I went offline and restarted my computer. The first thing I did after re booting was check "view statistics" with NIS. Normally the only connection open after re booting is "symproxysvc.exe". But there were 2 connections opened, "ms spool32.exe" and "symproxysvc.exe". I did a search for "ms spool32.exe" and found it in the windows folder along with 2 other files I never seen before, "MS SPOOL32.dat" and "MS SPOOL32k.dat". I checked properties and all 3 files were created at the time I double clicked on "Amy_orgasm.ram". I opened

Re: NORTON Firewall doesn't detect TROJAN, !!WARNING TROJAN ATTACHED!!

comp.security.firewalls: Re: NORTON Firewall doesn't detect TROJAN, !!WARNING TROJAN ATTACHED!!

"first_3sum.wri" again in MS Wordpad and highlighted "Amy_orgasm.ram" and selected "edit package". The appearance window said "Amy_orgasm.ram" but the content window said "copy of dynu.exe". "MS SPOOL32.dat" contains a list of .exe files I think "ms spool32.exe" is trying to shutdown. A few samples from "MS SPOOL32.dat">>>> (NAVAPW32.EXE, IAMAPP.EXE, ZONEALARM.EXE, VSHWIN32.EXE, REGEDIT.EXE, DRWATSON.EXE, SYSEDIT.EXE, NETSTAT.EXE, SCONFIG.EXE, GUARD.EXE, UPDATE.EXE, AUTOUPDATE.EXE, CLEANER.EXE, UPDATE.EXE, ANTI-TROJAN.EXE, WATCHDOG.EXE, BLACKICE.EXE, LUCOMSERVER.EXE, TASKMGR.EXE, GUARDDOG.EXE). "MS SPOOL32k.dat" contained by date and time all the programs that were opened and the keystrokes I made in those programs. I could see my sign on password, my social security number and password for my 401K web site. I'm lucky I blocked "ms spool32.exe" from connecting to the internet. I tried to delete the 3 new files but windows wouldn't let me. I checked the windows registry>>>> hkey_local_machine\software\microsoft\windows\currentversion\run and found a line for "ms spool32.exe". I deleted the entry but it comes back after I reboot and "ms spool32.exe" is loaded. The only way I could keep "ms spool32.exe" from loading and able to delete the 3 files that were created is if I do a system restore to an earlier point in time.

Before I deleted the files I did a "Scan with Norton AntiVirus" on the files>> "first_3sum.wri", "Amy_orgasm.ram" and "ms spool32.exe". Norton AntiVirus said they were all OK. I did an application scan and NIS did not detect that "ms spool32.exe" is internet enabled program. I think NIS should have detected the trojan when it was put on my hard drive and detected "ms spool32.exe" as an internet enabled application. You can tell by the logs that "ms spool32.exe" was trying to connect to the internet.

I hope Symantec will show more interest this time and tell me how to remove everything that the trojan put on my hard drive, registry, start, up files(etc.) and update your product to detect this trojan.

Symantec's reply to my first attempt below.

Date sent: Mon, 9 Dec 2002 03:12:03 UT
From: SecurityResponse@symantec.com
To: -----@prodigy.net
Subject: [CLOSING]: Symantec Security Response
Automation: Tracking #2291036

Below is a status update on your virus submission:

Date: December 8, 2002

Dear Watson Engler,

We have analyzed your submission. The following is a report of our findings for each file you have submitted:

Re: NORTON Firewall doesn't detect TROJAN, !!WARNING TROJAN ATTACHED!!

comp.security.firewalls: Re: NORTON Firewall doesn't detect TROJAN, !!WARNING TROJAN ATTACHED!!

filename: C:\temp\first_3sum.wri

machine:

result: This file is clean

Developer notes:

C:\temp\first_3sum.wri is a clean file.

We have determined that no virus exists on the samples provided.