Subject: Virus Scan Problem
Posted by Dave Camenisch on Tue, 03 May 2005 06:49:41 GMT
View Forum Message <> Reply to Message

Hello
I use(d) F-Prot (DOS) as my first virus scanner in NST. Today I realized that my second virus scanner (mcafee / outside of NST) catches more and more virus mails. I checked the filter setting and saw that the filtertest reports this:

```
May 03, 2005, 08:24:55 Session 0: (F-Prot Anti Virus) Executing: cmd /Q /D /C "C:\program
files\f-prot\F-PROT.EXE" /nofloppy /silent C:\DOKUME~1\ADMINI~1\LOKALE~1\Temp\FP0i.msg
/report=C:\DOKUME~1\ADMINI~1\LOKALE~1\Temp\FP0e.log
May 03, 2005, 08:25:14 Session 0: (F-Prot Anti Virus) Command line exit code is 255
May 03, 2005, 08:25:14 Session 0: (F-Prot Anti Virus) Rename file failed
May 03, 2005, 08:25:14 Session 0: (F-Prot Anti Virus) Command stderr output:
May 03, 2005, 08:25:14 Session 0: (F-Prot Anti Virus) Virus scanning report  -  3 May 2005 @
8:25
May 03, 2005, 08:25:14 Session 0: (F-Prot Anti Virus)
May 03, 2005, 08:25:14 Session 0: (F-Prot Anti Virus) F-PROT ANTIVIRUS
May 03, 2005, 08:25:14 Session 0: (F-Prot Anti Virus) Program version: 3.15b
May 03, 2005, 08:25:14 Session 0: (F-Prot Anti Virus) Engine version: 3.15.3
May 03, 2005, 08:25:14 Session 0: (F-Prot Anti Virus)
May 03, 2005, 08:25:14 Session 0: (F-Prot Anti Virus) VIRUS SIGNATURE FILES
May 03, 2005, 08:25:14 Session 0: (F-Prot Anti Virus) SIGN.DEF created 2 May 2005
May 03, 2005, 08:25:14 Session 0: (F-Prot Anti Virus) SIGN2.DEF created 2 May 2005
May 03, 2005, 08:25:14 Session 0: (F-Prot Anti Virus) MACRO.DEF created 2 May 2005
May 03, 2005, 08:25:14 Session 0: (F-Prot Anti Virus)
May 03, 2005, 08:25:14 Session 0: (F-Prot Anti Virus) Search:
C:\DOKUME~1\ADMINI~1\LOKALE~1\Temp\FP0i.msg
May 03, 2005, 08:25:14 Session 0: (F-Prot Anti Virus) Action: Report only
May 03, 2005, 08:25:14 Session 0: (F-Prot Anti Virus) Files: "Dumb" scan of all files
May 03, 2005, 08:25:14 Session 0: (F-Prot Anti Virus) Switches: /ARCHIVE /PACKED
/REPORT=C:\DOKUME~1\ADMINI~1\LOKALE~1\Temp\FP0e.log /SILENT /NOFLOPPY
May 03, 2005, 08:25:14 Session 0: (F-Prot Anti Virus) No viruses found in memory.
May 03, 2005, 08:25:14 Session 0: (F-Prot Anti Virus) Hard disk boot sectors were not scanned.
May 03, 2005, 08:25:14 Session 0: (F-Prot Anti Virus)
May 03, 2005, 08:25:14 Session 0: (F-Prot Anti Virus)
May 03, 2005, 08:25:14 Session 0: (F-Prot Anti Virus) Results of virus scanning:
May 03, 2005, 08:25:14 Session 0: (F-Prot Anti Virus)
May 03, 2005, 08:25:14 Session 0: (F-Prot Anti Virus) Files: 1
May 03, 2005, 08:25:14 Session 0: (F-Prot Anti Virus) MBRs: 0
May 03, 2005, 08:25:14 Session 0: (F-Prot Anti Virus) Boot sectors: 0
May 03, 2005, 08:25:14 Session 0: (F-Prot Anti Virus) Objects scanned: 0
May 03, 2005, 08:25:14 Session 0: (F-Prot Anti Virus)
May 03, 2005, 08:25:14 Session 0: (F-Prot Anti Virus) Time: 0:00
May 03, 2005, 08:25:14 Session 0: (F-Prot Anti Virus)
May 03, 2005, 08:25:14 Session 0: (F-Prot Anti Virus) No viruses or suspicious files/boot sectors
```

were found.
May 03, 2005, 08:25:14 Session 0: (F-Prot Anti Virus) Filter result is reject/delete (non-recoverable error)

-> "Rename file failed" ?

The same error happens when I try clamav instead of f-prot... I have no idea what it means and why this happens. In normal operation f-prot reports a timeout error in the NST log.

Regards
Dave

Subject: Re: Virus Scan Problem
Posted by support on Tue, 03 May 2005 10:25:22 GMT

View Forum Message <> Reply to Message

> -> "Rename file failed" ?

Filters have an input file, and an output file, e.g. FP2i and FP2o. For filters that do not modify mail content, the output file is created by renaming the input file.

Renaming can fail for a number of reasons, i.e. the output file already exists and it can't be deleted.
Whatever the reason, you need to check the access permissions in the temporary directory used by NoSpamToday!.

The temporary directory used is logged upon startup of NoSpamToday! in the log file.

To change the directory, set the TEMP or TMP environment variable.

Subject: Re: Virus Scan Problem
Posted by Heidner on Wed, 04 May 2005 22:27:52 GMT

View Forum Message <> Reply to Message

Another reason for rename failing is:

1) if your other scanner has autoprotect and it is enabled - it may be detecting the file while NST creates the "\temp*.msg" file. That would make F-Protect think that it was started without a file to scan. If this is happening you should be seeing files quarantined by your primary (non _Fprotect-DOS) scanner - and the files should have the same name pattern "\temp*.msg".

If this is happening you can solve that (at least with Symantec Corporate edition) by (two methods)

1)creating a new directory just for the NoSpamToday "msg" files.   Something like "\NST_temp" , then change your environment variables used by NST (and the command line option so that the "msg" file is written into this other directory. Finally change the autoprotect option on your primary scanner -- not to check files in the "\NST_temp" directory

2) the other method is to tell your primary scanner that has autoprotect to exclude checking files with the ".msg" extension.

Finally if it is autoprotect catching the virus - another option is to leave your current setup alone -- if you can affort the slight performance hit --- because would mean that every e-mail is actually getting checked twice before delivery to the mail server.

Subject: Re: Virus Scan Problem
Posted by Dave Camenisch on Fri, 06 May 2005 04:41:02 GMT

View Forum Message <> Reply to Message

The second virus scanner is not the problem (I disabled it for testing).

How can I change the "environement varibables"? Is that in a file?

I changed the command for F-Prot (DOS) to: "cmd /Q /D %SCANNER% /nofloppy /silent %IN%".
Now F-Prot seems to work again but I really don't know what missing "/C" and "/report=..." are for...
When I run the "Test with Sample Virus" now then I get an command line exit code "0".
With "/C" I get the exit code "255" and with "/report=%Err% an exit code "1".
What are the commands /Q /D /C and /report= for? And how relevant is the order of this commands?

-- Dave

Subject: Re: Virus Scan Problem
Posted by support on Fri, 06 May 2005 11:37:56 GMT

View Forum Message <> Reply to Message

> How can I change the "environement varibables"? Is that in a
> file?

Login with the account NoSpamToday! uses, from the start menu find settings -> system, find a tab named extras, or extended (or similar, you are never sure which depending on the OS version and language). There you can click on a button to bring up a dialog where you can change or add environment variables.
>
> I changed the command for F-Prot (DOS) to: "cmd /Q /D

> %SCANNER% /nofloppy /silent %IN%". Now F-Prot seems to work
> again but I really don't know what missing "/C" and
> "/report=..." are for...
> When I run the "Test with Sample Virus" now then I get an
> command line exit code "0".
> With "/C" I get the exit code "255" and with "/report=%Err%
> an exit code "1".
> What are the commands /Q /D /C and /report= for? And how
> relevant is the order of this commands?

/Q /D /C are options of the command line wrapper needed to run f-prot for DOS. if you delete the /C option, f-prot is not started at all, and the exit code can be anything. For a description of cmd's options, type "help cmd" in a command line window.

Your signature files are up-to-date, so there is no reason why f-prot should detect significantly less viruses than McAfee. You could try and capture one of the mails detected by McAfee only, and have a close look at it.

Use a mail storage filter for this, placed between f-prot and McAfee, and once you see in the log that McAfee found a virus not captured by f-prot, look up this file in the storage dir.

Do not forget to tell the virus scanners you may have installed to skip the storage dir, otherwise you won't find the mail there.

Subject: Re: Virus Scan Problem
Posted by Dave Camenisch on Fri, 06 May 2005 16:37:06 GMT

View Forum Message <> Reply to Message

> /Q /D /C are options of the command line wrapper needed to
> run f-prot for DOS. if you delete the /C option, f-prot is not
> started at all, and the exit code can be anything. For a
> description of cmd's options, type "help cmd" in a command line
> window.

I see "/C" is a must. That also explains why McAfee is catching so many viruses.

I run the Sample Virus Test in NST and here are the results with different settings:
(Environemet variable Temp and Tmp = "C:\temp" / McAfee disabled)

1.) cmd /Q /D /C %SCANNER% /nofloppy /silent %IN% /report=%ERR% (default settings)
First an empty DOS window opens and the header shows
- "C:\program files\f-prot316\F-Prot.EXE" /nofloppy /silent C:\temp\FP0i.msg /report=C:\temp\FP0e.log"
- then "F-Prot"
- and then "Nicht aktiv F-Prot" (not activ?).

When I close this window immediately then the output shows:

```
--
May 06, 2005, 17:45:39 Session 0: (F-Prot Anti Virus) Executing: cmd /Q /D /C "C:\program files\f-prot316\F-PROT.EXE" /nofloppy /silent C:\temp\FP0i.msg /report=C:\temp\FP0e.log
May 06, 2005, 17:45:41 Session 0: (F-Prot Anti Virus) Command line exit code is 255
May 06, 2005, 17:45:41 Session 0: (F-Prot Anti Virus) Command stderr output:
May 06, 2005, 17:45:41 Session 0: (F-Prot Anti Virus) Virus scanning report  -  6 May 2005 @ 17:45
May 06, 2005, 17:45:41 Session 0: (F-Prot Anti Virus)
May 06, 2005, 17:45:41 Session 0: (F-Prot Anti Virus) F-PROT ANTIVIRUS
May 06, 2005, 17:45:41 Session 0: (F-Prot Anti Virus) Program version: 3.16b
May 06, 2005, 17:45:41 Session 0: (F-Prot Anti Virus) Engine version: 3.16.6
May 06, 2005, 17:45:41 Session 0: (F-Prot Anti Virus)
May 06, 2005, 17:45:41 Session 0: (F-Prot Anti Virus) VIRUS SIGNATURE FILES
May 06, 2005, 17:45:41 Session 0: (F-Prot Anti Virus) SIGN.DEF created 5 May 2005
May 06, 2005, 17:45:41 Session 0: (F-Prot Anti Virus) SIGN2.DEF created 5 May 2005
May 06, 2005, 17:45:41 Session 0: (F-Prot Anti Virus) MACRO.DEF created 2 May 2005
May 06, 2005, 17:45:41 Session 0: (F-Prot Anti Virus)
May 06, 2005, 17:45:41 Session 0: (F-Prot Anti Virus) Search: C:\temp\FP0i.msg
May 06, 2005, 17:45:41 Session 0: (F-Prot Anti Virus) Action: Report only
May 06, 2005, 17:45:41 Session 0: (F-Prot Anti Virus) Files: "Dumb" scan of all files
May 06, 2005, 17:45:41 Session 0: (F-Prot Anti Virus) Switches: /ARCHIVE /PACKED /REPORT=C:\temp\FP0e.log /SILENT /NOFLOPPY
May 06, 2005, 17:45:41 Session 0: (F-Prot Anti Virus) No viruses found in memory.
May 06, 2005, 17:45:41 Session 0: (F-Prot Anti Virus) Hard disk boot sectors were not scanned.
May 06, 2005, 17:45:41 Session 0: (F-Prot Anti Virus)
May 06, 2005, 17:45:41 Session 0: (F-Prot Anti Virus) C:\TEMP\FP0I.MSG->eicar.com  Infection: EICAR_Test_File
May 06, 2005, 17:45:41 Session 0: (F-Prot Anti Virus)
May 06, 2005, 17:45:41 Session 0: (F-Prot Anti Virus) Results of virus scanning:
May 06, 2005, 17:45:41 Session 0: (F-Prot Anti Virus)
May 06, 2005, 17:45:41 Session 0: (F-Prot Anti Virus) Files: 1
May 06, 2005, 17:45:41 Session 0: (F-Prot Anti Virus) MBRs: 0
May 06, 2005, 17:45:41 Session 0: (F-Prot Anti Virus) Boot sectors: 0
May 06, 2005, 17:45:41 Session 0: (F-Prot Anti Virus) Objects scanned: 2
May 06, 2005, 17:45:41 Session 0: (F-Prot Anti Virus) Infected: 1
May 06, 2005, 17:45:41 Session 0: (F-Prot Anti Virus) Suspicious: 0
May 06, 2005, 17:45:41 Session 0: (F-Prot Anti Virus) Disinfected: 0
May 06, 2005, 17:45:41 Session 0: (F-Prot Anti Virus) Deleted: 0
May 06, 2005, 17:45:41 Session 0: (F-Prot Anti Virus) Renamed: 0
May 06, 2005, 17:45:41 Session 0: (F-Prot Anti Virus)
May 06, 2005, 17:45:41 Session 0: (F-Prot Anti Virus) Time: 0:00
May 06, 2005, 17:45:41 Session 0: (F-Prot Anti Virus) Filter result is accept/deliver (unknown result)
--
```

When I wait a minute before closing the DOS window the output shows the same but line 2 is:

```
May 06, 2005, 17:49:42 Session 0: (F-Prot Anti Virus) Command execution timed out
```

2.) `cmd /Q /D /C %SCANNER% /nofloppy /silent %IN%`

```
--
May 06, 2005, 18:01:22 Session 0: (F-Prot Anti Virus) Executing: cmd /Q /D /C "C:\program
files\f-prot316\F-PROT.EXE" /nofloppy /silent C:\temp\FP0i.msg
May 06, 2005, 18:02:00 Session 0: (F-Prot Anti Virus) Command line exit code is 255
May 06, 2005, 18:02:00 Session 0: (F-Prot Anti Virus) Filter result is accept/deliver (unknown
result)
--
```

When I wait a minute:

```
--
May 06, 2005, 18:02:47 Session 0: (F-Prot Anti Virus) Executing: cmd /Q /D /C "C:\program
files\f-prot316\F-PROT.EXE" /nofloppy /silent C:\temp\FP0i.msg
May 06, 2005, 18:03:48 Session 0: (F-Prot Anti Virus) Command execution timed out
May 06, 2005, 18:03:48 Session 0: (F-Prot Anti Virus) Filter result is accept/deliver (unknown
result)
--
```

3.) `cmd /Q /D %SCANNER% /nofloppy /silent %IN%`
No DOS window opens!

```
--
May 06, 2005, 18:05:37 Session 0: (F-Prot Anti Virus) Executing: cmd /Q /D "C:\program
files\f-prot316\F-PROT.EXE" /nofloppy /silent C:\temp\FP0i.msg
May 06, 2005, 18:05:38 Session 0: (F-Prot Anti Virus) Command line exit code is 0
May 06, 2005, 18:05:38 Session 0: (F-Prot Anti Virus) Filter result is accept/deliver
--
```

4.) `cmd /Q /D %SCANNER% /nofloppy /silent %IN% /report=%ERR%`

```
--
May 06, 2005, 18:17:06 Session 0: (F-Prot Anti Virus) Executing: cmd /Q /D "C:\program
files\f-prot316\F-PROT.EXE" /nofloppy /silent C:\temp\FP0i.msg /report=C:\temp\FP0e.log
May 06, 2005, 18:17:07 Session 0: (F-Prot Anti Virus) Command line exit code is 1
May 06, 2005, 18:17:07 Session 0: (F-Prot Anti Virus) Cannot open file C:\temp\FP0e.log
mode=read (No such file or directory)
May 06, 2005, 18:17:07 Session 0: (F-Prot Anti Virus) Filter result is accept/deliver (unknown
result)
--
```

Directory "C:\temp" exists and access privileges are ok!

The big question for me is: why does F-Prot runs in a timeout with the default settings?
F-Prot has worked fine until I updatet it from version 3.12 to 3.16. But also when I switch back to version 3.12 it still doesn't work anymore.

-- Dave

Subject: Re: Virus Scan Problem
Posted by Heidner on Sat, 07 May 2005 05:42:54 GMT
View Forum Message <> Reply to Message

You mentioned that you had tried ClamAV,   clamav uses a daemon that must be running else you get time out errors (clamd - started with a .bat file).   Was the daemon running?

Does F-Prot Antivirus also expect to have a scanning daemon running in the background?

Subject: Re: Virus Scan Problem
Posted by Dave Camenisch on Sat, 07 May 2005 08:23:03 GMT
View Forum Message <> Reply to Message

> You mentioned that you had tried ClamAV,   clamav uses a
> daemon that must be running else you get time out errors (clamd
> - started with a .bat file).   Was the daemon running?

ClamAV is another big problem. I installed it, setup a filter with default settings (I did not startet anything) and run the Sample Virus Test. Everything looks ok. When I look at the log file it seems that ClamAV is working correctly:

```
--
May 07, 2005, 08:01:32 Session 0: (Attachment Filter) From: xxxx@bluewin.ch
May 07, 2005, 08:01:32 Session 0: (Attachment Filter) Subject: testmail
May 07, 2005, 08:01:32 Session 0: (Attachment Filter) To: dave.camenisch@capslock.ch
May 07, 2005, 08:01:32 Session 0: Received end of data, mail size 1kB
May 07, 2005, 08:01:32 Session 0: (Attachment Filter) Filter result is accept/deliver
May 07, 2005, 08:01:32 Session 0: (Spam Trap) No action
May 07, 2005, 08:01:35 Session 0: (Clam Anti Virus) Filter result is accept/deliver
May 07, 2005, 08:01:45 Session 0: (SpamAssassin) Filter result is accept/deliver
May 07, 2005, 08:01:45 Session 0: (SpamAssassin) Spam score: 2.2
--
```

BUT THEN I realized that the mails are never reaching the mail server!!!
I don't know what happens because the log seems to be ok. Fact is that when I delete the ClamAV filter the mails are coming in again.

A very frustrating situation... :(

-- Dave

Subject: Re: Virus Scan Problem
Posted by Heidner on Sat, 07 May 2005 20:10:25 GMT

View Forum Message <> Reply to Message

Strange... it doesn't look like CLAMAV is really running... you should be seeing something like:

```
May 06, 2005, 00:01:37 Session 0: (Attachment Filter) Subject: Get up to a 300
May 06, 2005, 00:01:37 Session 0: Received end of data, mail size 5kB
May 06, 2005, 00:01:37 Session 0: (Attachment Filter) Filter result is accept/deliver
May 06, 2005, 00:01:37 Session 0: (Spam Trap) No action
May 06, 2005, 00:01:37 Session 0: (Clam Anti Virus) Executing:
D:\clamav-devel\bin\clamdscan.exe "D:\WINNT\ClamAV0i.msg" --mbox --no-summary
--mail-follow-urls
May 06, 2005, 00:01:38 Session 0: (Clam Anti Virus) Command line exit code is 0
May 06, 2005, 00:01:38 Session 0: (Clam Anti Virus) Filter result is accept/deliver
May 06, 2005, 00:01:40 Session 0: (Mail Storage) Message cached in
D:\TEMP\nospamtoday\the-count_00001B0F.msg
May 0
```

Your log file doesn't have anything about clamav executing...

Which version of CLAMAV did you install? The windows or cmd line version?

You should also probably send NST support more information about your mail server config, i.e. windows version/os, nst config file.

Also are you running a program like BlackIce Server? If so you need to run new baselines when you add software - otherwise BlackIce will terminate the application (like clamav) as soon as it is loaded into memory but before it actually executes.

Subject: Re: Virus Scan Problem
Posted by support on Mon, 09 May 2005 12:29:25 GMT

View Forum Message <> Reply to Message

[...]

> The big question for me is: why does F-Prot runs in a timeout
> with the default settings?
> F-Prot has worked fine until I updatet it from version 3.12
> to 3.16. But also when I switch back to version 3.12 it still
> doesn't work anymore.

With DOS programs, you can tell windows to close the associated window after the program finishes. You did this probably for the old version, but you forgot to do so for the new version, now both versions time out, because the window is not closed.

To remedy this, use the Windows explorer to find F-PROT.EXE, choose properties from the popup menu, and configure Windows to close the program window when F-Prot has finished.

Note that this only affects F-Prot's behavior when testing in the admin app. The NoSpamToday! service is not interactive, and thus no window is opened, and thus there is no timeout problem.