Subject: AntiVirus not working right?
Posted by smorris on Thu, 16 Dec 2004 16:13:44 GMT
View Forum Message <> Reply to Message

I have installed F-Prot AV which is one of the "preferred" AV programs. I am repeatedly getting failures and therefore no scans.

Log info:

Dec 16, 2004, 11:02:46 Session 0: (F-Prot Anti Virus) Cannot open file
C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\FP0e.log mode=read (No such file or directory)
Dec 16, 2004, 11:02:46 Session 0: (F-Prot Anti Virus) Filter result is accept/deliver
Dec 16, 2004, 11:02:46 Session 0: Incoming mail action: accept/deliver (marked as junk)
Dec 16, 2004, 11:02:54 Session 1: (SpamAssassin) Filter result is accept/deliver (marked as junk)
Dec 16, 2004, 11:02:54 Session 1: (SpamAssassin) Spam score: 15.7
Dec 16, 2004, 11:02:55 Session 1: (F-Prot Anti Virus) Cannot open file
C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\FP1e.log mode=read (No such file or directory)
Dec 16, 2004, 11:02:55 Session 1: (F-Prot Anti Virus) Filter result is accept/deliver
Dec 16, 2004, 11:02:55 Session 1: Incoming mail action: accept/deliver (marked as junk)
Dec 16, 2004, 11:05:53 Session 0: (Attachment Filter) Subject: RE: NBAR for Security Filtering
Dec 16, 2004, 11:05:53 Session 0: (Attachment Filter) From: "Church, Chuck"
Dec 16, 2004, 11:05:53 Session 0: (Attachment Filter) To: "ccie2be" , "Group Study"
Dec 16, 2004, 11:05:53 Session 0: (Attachment Filter)
Dec 16, 2004, 11:05:53 Session 0: Received end of data, mail size 12kB
Dec 16, 2004, 11:05:53 Session 0: (Attachment Filter) Filter result is accept/deliver
Dec 16, 2004, 11:06:07 Session 0: (SpamAssassin) Filter result is accept/deliver
Dec 16, 2004, 11:06:07 Session 0: (SpamAssassin) Spam score: 4.5
Dec 16, 2004, 11:06:08 Session 0: (F-Prot Anti Virus) Cannot open file
C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\FP0e.log mode=read (No such file or directory)
Dec 16, 2004, 11:06:08 Session 0: (F-Prot Anti Virus) Filter result is accept/deliver
Dec 16, 2004, 11:06:08 Session 0: Incoming mail action: accept/deliver
Dec 16, 2004, 11:07:59 Session 0: (Attachment Filter) From: "Joshua Mims"
Dec 16, 2004, 11:07:59 Session 0: (Attachment Filter) To:
Dec 16, 2004, 11:07:59 Session 0: (Attachment Filter) Subject: RE: Send the last email.
Dec 16, 2004, 11:08:00 Session 0: Received end of data, mail size 2kB
Dec 16, 2004, 11:08:00 Session 0: (Attachment Filter) Filter result is accept/deliver
Dec 16, 2004, 11:08:06 Session 0: (SpamAssassin) Filter result is accept/deliver
Dec 16, 2004, 11:08:06 Session 0: (SpamAssassin) Spam score: 1.0
Dec 16, 2004, 11:08:07 Session 0: (F-Prot Anti Virus) Cannot open file
C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\FP0e.log mode=read (No such file or directory)
Dec 16, 2004, 11:08:07 Session 0: (F-Prot Anti Virus) Filter result is accept/deliver
Dec 16, 2004, 11:08:07 Session 0: Incoming mail action: accept/deliver

Now, the directory info is all passed along by NST. So as far as I know, there's no way to specify or control this. It simply looks like NST is not creating the file and therefore F-Prot is confused about it all.

Please advise.

Subject: Re: AntiVirus not working right?
Posted by support on Fri, 17 Dec 2004 11:07:49 GMT
View Forum Message <> Reply to Message

> I have installed F-Prot AV which is one of the "preferred" AV
> programs. I am repeatedly getting failures and therefore no
> scans.

[...]

> Dec 16, 2004, 11:02:55 Session 1: (F-Prot Anti Virus) Cannot
> open file C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\FP1e.log mode=read
> (No such file or directory)
> Dec 16, 2004, 11:02:55 Session 1: (F-Prot Anti Virus) Filter
> result is accept/deliver

This is the "log filter error output" option of NoSpamToday! trying to read f-prot's report file (if you are using the default configuration). The filter itself seems to be running, you would not see the accept/deliver filtering result otherwise.

It should not happen nonetheless. Try "test with sample virus" and "test with sample spam" in the antivirus setup dialog, and do some experimenting with f-prot in a command line window.

BTW, enabling detailed logging writes the command line actually executed to the log.

Subject: Re: AntiVirus not working right?
Posted by smorris on Fri, 17 Dec 2004 14:10:47 GMT
View Forum Message <> Reply to Message

I would agree with the part that this should not happen anyway. :)

The command line is really what the NST config put in there. As far as the directory goes, the directory exists, so there's no reason it can't work.

Is there any way to specify where NST will place the file in order to be scanned by the AV program?

Detailed log:
Dec 17, 2004, 08:59:51 Session 1020: Connection from 127.0.0.1 accepted on 127.0.0.1:8086
Dec 17, 2004, 09:00:05 Session 0: Connection from 208.158.37.2 accepted on 208.158.37.23:25
Dec 17, 2004, 09:00:05 Session 0: 220 schlep.emanon.com (NT1887.00.097ced12) ready for ESMTP transfer
Dec 17, 2004, 09:00:05 Session 0: EHLO emanon.com
Dec 17, 2004, 09:00:05 Session 0: 250-schlep.emanon.com Hello spamrelay.emanon.com [208.158.37.23], pleased to meet you

Dec 17, 2004, 09:00:05 Session 0: 250-VRFY
Dec 17, 2004, 09:00:05 Session 0: 250-ENHANCEDSTATUSCODES
Dec 17, 2004, 09:00:05 Session 0: 250-8BITMIME
Dec 17, 2004, 09:00:05 Session 0: 250-ETRN
Dec 17, 2004, 09:00:05 Session 0: 250-DSN
Dec 17, 2004, 09:00:05 Session 0: 250-XRCPTLIMIT 50
Dec 17, 2004, 09:00:05 Session 0: 250-XAUD 789179kw4632313722188 0.9
Dec 17, 2004, 09:00:05 Session 0: 250 HELP
Dec 17, 2004, 09:00:05 Session 0: QUIT
Dec 17, 2004, 09:00:05 Session 0: 221 2.5.0 Goodbye spamrelay.emanon.com
Dec 17, 2004, 09:00:05 Session 0: Connection from 208.158.37.2 closed
Dec 17, 2004, 09:00:29 Session 0: Connection from 66.63.170.45 accepted on 208.158.37.23:25
Dec 17, 2004, 09:00:29 Session 0: Connection reset by client (recv failed)
Dec 17, 2004, 09:00:29 Session 0: Connection from 66.63.170.45 closed
Dec 17, 2004, 09:00:49 Session 0: Connection from 201.135.109.196 accepted on
208.158.37.23:25
Dec 17, 2004, 09:00:49 Session 0: 220 schlep.emanon.com (NT1887.00.097ced12) ready for
ESMTP transfer
Dec 17, 2004, 09:00:52 Session 0: HELO dsl-201-135-109-196.prod-infinitum.com.mx
Dec 17, 2004, 09:00:52 Session 0: 250 schlep.emanon.com spamrelay.emanon.com
Dec 17, 2004, 09:00:55 Session 0: MAIL FROM:
Dec 17, 2004, 09:00:56 Session 0: 250 OK.
Dec 17, 2004, 09:01:00 Session 0: RCPT TO:
Dec 17, 2004, 09:01:00 Session 0: 250 OK.
Dec 17, 2004, 09:01:04 Session 0: DATA
Dec 17, 2004, 09:01:04 Session 0: 354 Start mail input; end with .
Dec 17, 2004, 09:01:07 Session 1: Connection from 218.71.45.159 accepted on 208.158.37.23:25
Dec 17, 2004, 09:01:07 Session 1: 220 schlep.emanon.com (NT1887.00.097ced12) ready for
ESMTP transfer
Dec 17, 2004, 09:01:10 Session 1: EHLO curucam.de
Dec 17, 2004, 09:01:10 Session 1: 250-schlep.emanon.com Hello spamrelay.emanon.com
[208.158.37.23], pleased to meet you
Dec 17, 2004, 09:01:10 Session 1: 250-VRFY
Dec 17, 2004, 09:01:10 Session 1: 250-ENHANCEDSTATUSCODES
Dec 17, 2004, 09:01:10 Session 1: 250-8BITMIME
Dec 17, 2004, 09:01:10 Session 1: 250-ETRN
Dec 17, 2004, 09:01:10 Session 1: 250-DSN
Dec 17, 2004, 09:01:10 Session 1: 250-XRCPTLIMIT 50
Dec 17, 2004, 09:01:10 Session 1: 250-XAUD 789179kw15632513042191 0.9
Dec 17, 2004, 09:01:10 Session 1: 250 HELP
Dec 17, 2004, 09:01:11 Session 0: (Attachment Filter) From: "Toby Bermudez"
Dec 17, 2004, 09:01:11 Session 0: (Attachment Filter) To: "Orion"
Dec 17, 2004, 09:01:11 Session 0: (Attachment Filter) Subject: i got it all here
Dec 17, 2004, 09:01:11 Session 0: Received end of data, mail size 2kB
Dec 17, 2004, 09:01:11 Session 0: (Attachment Filter) Filter result is accept/deliver
Dec 17, 2004, 09:01:11 SpamAssassin DNS server(s): 208.158.37.12 208.158.37.10
Dec 17, 2004, 09:01:11 Session 0: (SpamAssassin) Executing: sa\spamassassin.exe -x -c
"sa\ruleset" -e 255

Dec 17, 2004, 09:01:11 Session 1: MAIL FROM:

Dec 17, 2004, 09:01:14 Session 0: (SpamAssassin) Command line exit code is 255

Dec 17, 2004, 09:01:14 Session 0: (SpamAssassin) Filter result is accept/deliver (marked as junk)

Dec 17, 2004, 09:01:14 Session 0: (SpamAssassin) Spam score: 13.5

Dec 17, 2004, 09:01:14 Session 0: (F-Prot Anti Virus) Executing: cmd /Q /D /C "c:\program files\fsi\f-prot\fpcmd.exe" /nofloppy /silent C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\FP0i.msg /report=C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\FP0e.log

Dec 17, 2004, 09:01:15 Session 0: (F-Prot Anti Virus) Command line exit code is 0

Dec 17, 2004, 09:01:15 Session 0: (F-Prot Anti Virus) Cannot open file C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\FP0e.log mode=read (No such file or directory)

Dec 17, 2004, 09:01:15 Session 0: (F-Prot Anti Virus) Filter result is accept/deliver

Dec 17, 2004, 09:01:15 Session 0: Incoming mail action: accept/deliver (marked as junk)

Dec 17, 2004, 09:01:16 Session 0: 250 Received message cigudaaa OK.

Dec 17, 2004, 09:01:21 Session 0: QUIT

Dec 17, 2004, 09:01:21 Session 0: 221 Goodbye spamrelay.emanon.com

Dec 17, 2004, 09:01:21 Session 0: Connection from 201.135.109.196 closed

Dec 17, 2004, 09:01:31 Session 1: Connection closed by client

Dec 17, 2004, 09:01:31 Session 1: Connection from 218.71.45.159 closed

Dec 17, 2004, 09:01:40 Session 0: Connection from 68.250.191.143 accepted on 208.158.37.23:25

Dec 17, 2004, 09:01:40 Session 0: 220 schlep.emanon.com (NT1887.00.097ced12) ready for ESMTP transfer

Dec 17, 2004, 09:01:41 Session 0: EHLO dmforum.dk

Dec 17, 2004, 09:01:41 Session 0: 250-schlep.emanon.com Hello spamrelay.emanon.com [208.158.37.23], pleased to meet you

Dec 17, 2004, 09:01:41 Session 0: 250-VRFY

Dec 17, 2004, 09:01:41 Session 0: 250-ENHANCEDSTATUSCODES

Dec 17, 2004, 09:01:41 Session 0: 250-8BITMIME

Dec 17, 2004, 09:01:41 Session 0: 250-ETRN

Dec 17, 2004, 09:01:41 Session 0: 250-DSN

Dec 17, 2004, 09:01:41 Session 0: 250-XRCPTLIMIT 50

Dec 17, 2004, 09:01:41 Session 0: 250-XAUD 789179kw59335813722192 0.9

Dec 17, 2004, 09:01:41 Session 0: 250 HELP

Dec 17, 2004, 09:01:41 Session 0: MAIL FROM:

Dec 17, 2004, 09:02:01 Session 0: Connection closed by client

Dec 17, 2004, 09:02:01 Session 0: Connection from 68.250.191.143 closed

Dec 17, 2004, 09:02:02 Session 0: Connection from 83.38.95.72 accepted on 208.158.37.23:25

Dec 17, 2004, 09:02:02 Session 0: 220 schlep.emanon.com (NT1887.00.097ced12) ready for ESMTP transfer

Dec 17, 2004, 09:02:03 Session 0: EHLO yanos.slavneft.ru

Dec 17, 2004, 09:02:03 Session 0: 250-schlep.emanon.com Hello spamrelay.emanon.com [208.158.37.23], pleased to meet you

Dec 17, 2004, 09:02:03 Session 0: 250-VRFY

Dec 17, 2004, 09:02:03 Session 0: 250-ENHANCEDSTATUSCODES

Dec 17, 2004, 09:02:03 Session 0: 250-8BITMIME

Dec 17, 2004, 09:02:03 Session 0: 250-ETRN

Dec 17, 2004, 09:02:03 Session 0: 250-DSN

Dec 17, 2004, 09:02:03 Session 0: 250-XRCPTLIMIT 50

Dec 17, 2004, 09:02:03 Session 0: 250-XAUD 789179kw42132013042193 0.9
Dec 17, 2004, 09:02:03 Session 0: 250 HELP
Dec 17, 2004, 09:02:04 Session 0: MAIL FROM:
Dec 17, 2004, 09:02:05 Session 1: Connection from 208.158.37.2 accepted on 208.158.37.23:25
Dec 17, 2004, 09:02:05 Session 1: 220 schlep.emanon.com (NT1887.00.097ced12) ready for ESMTP transfer
Dec 17, 2004, 09:02:05 Session 1: EHLO emanon.com
Dec 17, 2004, 09:02:05 Session 1: 250-schlep.emanon.com Hello spamrelay.emanon.com [208.158.37.23], pleased to meet you
Dec 17, 2004, 09:02:05 Session 1: 250-VRFY
Dec 17, 2004, 09:02:05 Session 1: 250-ENHANCEDSTATUSCODES
Dec 17, 2004, 09:02:05 Session 1: 250-8BITMIME
Dec 17, 2004, 09:02:05 Session 1: 250-ETRN
Dec 17, 2004, 09:02:05 Session 1: 250-DSN
Dec 17, 2004, 09:02:05 Session 1: 250-XRCPTLIMIT 50
Dec 17, 2004, 09:02:05 Session 1: 250-XAUD 789179kw32832313762194 0.9
Dec 17, 2004, 09:02:05 Session 1: 250 HELP
Dec 17, 2004, 09:02:05 Session 1: QUIT
Dec 17, 2004, 09:02:05 Session 1: 221 2.5.0 Goodbye spamrelay.emanon.com
Dec 17, 2004, 09:02:05 Session 1: Connection from 208.158.37.2 closed
Dec 17, 2004, 09:02:23 Session 0: Connection closed by client
Dec 17, 2004, 09:02:23 Session 0: Connection from 83.38.95.72 closed
Dec 17, 2004, 09:02:45 Session 0: Connection from 131.103.218.79 accepted on 208.158.37.23:25
Dec 17, 2004, 09:02:45 Session 0: 220 schlep.emanon.com (NT1887.00.097ced12) ready for ESMTP transfer
Dec 17, 2004, 09:02:45 Session 0: HELO mail15a.boca15-verio.com
Dec 17, 2004, 09:02:45 Session 0: 250 schlep.emanon.com spamrelay.emanon.com
Dec 17, 2004, 09:02:45 Session 0: MAIL FROM:
Dec 17, 2004, 09:02:45 Session 0: 250 OK.
Dec 17, 2004, 09:02:45 Session 0: RCPT TO:
Dec 17, 2004, 09:02:45 Session 0: 250 OK.
Dec 17, 2004, 09:02:45 Session 0: DATA
Dec 17, 2004, 09:02:45 Session 0: 354 Start mail input; end with .
Dec 17, 2004, 09:02:45 Session 0: (Attachment Filter) From: "Bob Denton"
Dec 17, 2004, 09:02:45 Session 0: (Attachment Filter) To:
Dec 17, 2004, 09:02:45 Session 0: (Attachment Filter) Subject: Home Lab
Dec 17, 2004, 09:02:45 Session 0: Received end of data, mail size 4kB
Dec 17, 2004, 09:02:45 Session 0: (Attachment Filter) Filter result is accept/deliver
Dec 17, 2004, 09:02:45 Session 0: (SpamAssassin) Executing: sa\spamassassin.exe -x -c "sa\ruleset" -e 255
Dec 17, 2004, 09:02:59 Session 0: (SpamAssassin) Command line exit code is 0
Dec 17, 2004, 09:02:59 Session 0: (SpamAssassin) Filter result is accept/deliver
Dec 17, 2004, 09:02:59 Session 0: (SpamAssassin) Spam score: 5.6
Dec 17, 2004, 09:02:59 Session 0: (F-Prot Anti Virus) Executing: cmd /Q /D /C "c:\program files\fsi\f-prot\fpcmd.exe" /nofloppy /silent C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\FP0i.msg /report=C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\FP0e.log
Dec 17, 2004, 09:03:00 Session 0: (F-Prot Anti Virus) Command line exit code is 0

Dec 17, 2004, 09:03:00 Session 0: (F-Prot Anti Virus) Cannot open file
C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\FP0e.log mode=read (No such file or directory)
Dec 17, 2004, 09:03:00 Session 0: (F-Prot Anti Virus) Filter result is accept/deliver
Dec 17, 2004, 09:03:00 Session 0: Incoming mail action: accept/deliver
Dec 17, 2004, 09:03:01 Session 0: 250 Received message eigudaaa OK.
Dec 17, 2004, 09:03:01 Session 0: QUIT
Dec 17, 2004, 09:03:01 Session 0: 221 Goodbye spamrelay.emanon.com

---

Subject: Re: AntiVirus not working right?
Posted by support on Mon, 20 Dec 2004 10:08:52 GMT
View Forum Message <> Reply to Message

> Executing: cmd /Q /D /C "c:\program files\fsi\f-prot\fpcmd.exe"
> /nofloppy /silent C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\FP0i.msg
> /report=C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\FP0e.log

Something is wrong with the command line: With f-prot for Windows you do not need the cmd
wrapper, it is only needed for the DOS version. It could be that cmd is unable to start the scanner,
and for this reason no report file exists. Also in your case the exit code 0, which looks as if it is
working, would be in fact cmd's exit code, and not to the scanner's exit code.

Best delete this filter, and create it anew, the latest version of NoSpamToday! has two separate
configurations ready for f-prot for DOS and f-prot for Windows. Maybe you were starting out with a
pre-2.0.2.3 version. With fpcmd, choose the "f-prot for Windows" configuration.

Subject: Re: AntiVirus not working right?
Posted by smorris on Mon, 20 Dec 2004 14:28:37 GMT
View Forum Message <> Reply to Message

Ahhh... Very cool. yes, I'm running 2.0.2.3, but the filter was configured in an earlier version that
did not make that distinction!

but it has been eliminated and re-created, and appears to work now!

Thanks!

Scott

Subject: Re: AntiVirus not working right?
Posted by woddel on Tue, 21 Dec 2004 11:28:59 GMT
View Forum Message <> Reply to Message

hmmm... similar problem here. but i found out some more.

f-prot DOS somehow can not write into the temp directory
C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\FP0e.log

i copied the whole command and rewrote it to test:
cmd /Q /D /C "c:\program files\fsi\f-prot\fpcmd.exe"
/nofloppy /silent C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\FP0i.msg
/report=C:\FP0e.log

and then it worked (f-prot) by writing the log file. but of course when i tried this in nst, this does
not work as nst hardcodedly searches for the logfile in this path (the %err% variable, which seems
can not be changed. is there a workaround for this? can the global temp-directory somehow be
set inside nst config?

this, as the dos-version is free and the windows is not... :)

[...]
> cmd /Q /D /C "c:\program files\fsi\f-prot\fpcmd.exe"
> /nofloppy /silent C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\FP0i.msg
> /report=C:\FP0e.log

I believe this is half-broken, the DOS versions scanner name is f-prot.exe, if I am not mistaken.
So it looks like you are trying to use the Windows scanner in an unnecessary cmd wrapper. Again,
create the filter anew with the latest version.

[...]
> is there a
> workaround for this? can the global temp-directory somehow be
> set inside nst config?

You can set the temporary directory used by NoSpamToday! by setting one of the environment
variables TMP or TEMP in the account used by the service.

[...]
> this, as the dos-version is free and the windows is not...

but only for private use, if I remember the licensing conditions correctly...