Subject: NST and Sophos

Posted by declassified on Tue, 16 Aug 2005 19:00:01 GMT

View Forum Message <> Reply to Message

Hi All,

has anyone got any experience setting up anti virus filter with Sophos?

The problem I've encountered is that Sophos always returns exit code '0' when used in conjunction with NST. Weather is send a test virus message or test spam message the exit code is the same. Common sense tells me it shouldn't be like that. Moreover, when I use Sophos in DOS, it happily detects virus in test file I used for NST. My command line sintax for anti virus filter looks like this:

```
"C:\Program Files\Sophos\Sophos Anti-Virus\sav32cli.exe" "%IN%"
```

When I look at console output in NST I can see Sophos responses but the virus is simply not detected. Here's what I get.

```
Sophos Anti-Virus
Version 3.86.0 [Win32/Intel]
Virus data version 3.96, August 2005
Includes detection for 108398 viruses, trojans and worms
Copyright (c) 1989-2005 Sophos Plc, www.sophos.com
System time 19:37:15, System date 16 August 2005
IDE directory is: C:\Program Files\Sophos\Sophos Anti-Virus
Using IDE file ablnk-ae.ide
...
Using IDE file zotob-c.ide
Quick Scanning

1 file swept in 2 seconds.
No viruses were discovered.
Ending Sophos Anti-Virus.
```

Log output on the filter configuration test screen looks like this:

```
Aug 16, 2005, 19:37:13 Session 0: (Anti Virus) Executing: "C:\Program Files\Sophos\Sophos Anti-Virus\sav32cli.exe" "C:\DOCUME~1\admin\LOCALS~1\Temp\AV0i.msg"
Aug 16, 2005, 19:37:15 Session 0: (Anti Virus) Command line exit code is 0
Aug 16, 2005, 19:37:15 Session 0: (Anti Virus) Filter result is accept/deliver
```

To add insult to the injury even when I apply settings with av filter accepting all messages irrespective of the exit code, I can't see av filter being used by NST at all. However, I do see messages traversing attachment filter and spam assassin filter. The av filter is the last one in the chain but it doesn't seem to be used by NST.

Needless to say, this is becoming a nightmare. I would greatly appreciate if someone could suggest a possible solution or perhaps share some thoughts.

Thanks

Subject: Re: NST and Sophos
Posted by support on Thu, 18 Aug 2005 09:14:10 GMT
View Forum Message <> Reply to Message

declassified wrote:

> Hi All,
>
> has anyone got any experience setting up anti virus filter with
> Sophos?
>
> The problem I've encountered is that Sophos always returns exit
> code '0' when used in conjunction with NST. Weather is send a
> test virus message or test spam message the exit code is the
> same. Common sense tells me it shouldn't be like that.
> Moreover, when I use Sophos in DOS, it happily detects virus in
> test file I used for NST. My command line sintax for anti virus
> filter looks like this:
> "C:\Program Files\Sophos\Sophos Anti-Virus\sav32cli.exe" "%IN%"
>
>
> When I look at console output in NST I can see Sophos responses
> but the virus is simply not detected. Here's what I get.
>
> Sophos Anti-Virus
> Version 3.86.0 [Win32/Intel]
> Virus data version 3.96, August 2005
> Includes detection for 108398 viruses, trojans and worms
> Copyright (c) 1989-2005 Sophos Plc, www.sophos.com
> System time 19:37:15, System date 16 August 2005
> IDE directory is: C:\Program Files\Sophos\Sophos Anti-Virus
> Using IDE file ablnk-ae.ide
> ...
> Using IDE file zotob-c.ide
> Quick Scanning
>
> 1 file swept in 2 seconds.
> No viruses were discovered.
> Ending Sophos Anti-Virus.

>
>
> Log output on the filter configuration test screen looks like
> this:
>
> Aug 16, 2005, 19:37:13 Session 0: (Anti Virus) Executing:
> "C:\Program Files\Sophos\Sophos Anti-Virus\sav32cli.exe"
> "C:\DOCUME~1\admin\LOCALS~1\Temp\AV0i.msg"
> Aug 16, 2005, 19:37:15 Session 0: (Anti Virus) Command line
> exit code is 0
> Aug 16, 2005, 19:37:15 Session 0: (Anti Virus) Filter result is
> accept/deliver
>
>
> To add insult to the injury even when I apply settings with av
> filter accepting all messages irrespective of the exit code, I
> can't see av filter being used by NST at all. However, I do see
> messages traversing attachment filter and spam assassin filter.
> The av filter is the last one in the chain but it doesn't seem
> to be used by NST.
>
> Needless to say, this is becoming a nightmare. I would greatly
> appreciate if someone could suggest a possible solution or
> perhaps share some thoughts.

Both antivirus and SpamAssassin do not execute the filter, if the filter is unable to make the result "worse" than earlier filters. So if the worst your filter can do is "accept/deliver", it usually won't get started.

Assign "reject/delete" to exit code e.g. 100, and your antivirus filter will be started, even if this exit code never ever appears.

I don't know a lot about Sophos, but maybe it can be configured to sanitize messages. This way you can get rid of viruses, even if Sophos always returns exit code 0.

Please let us know how it works, this way we can widen our knowledge and maybe help other users in the future with similar problems.