

Re: Is this some sort of virus?

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2004-03/0476.html>

From: N. Miller (*nsm_at_blackhole.aosake.net*)

Date: 03/06/04

Date: Sat, 6 Mar 2004 14:35:48 -0800

In article <X9b2c.21077\$yZ1.580@newsread2.news.pas.earthlink.net>, notdisclosed@example.com says...

- > *I have not found that Norton AntiVirus has any bad effect on Microsoft*
- > *Outlook.*

I wouldn't know about MSOL, it is MSOE where the problem seems to crop up.

- > *If it, or any other AV program does, then it should be an issue*
- > *for the publisher of the AV program and Microsoft to resolve, not a reason*
- > *for "MVP's" to recommend not using it...*

It appears that Symantec has made some changes which make the MVP advice moot, now. Indeed, one of them has pointed this out in a very recent message; dated March 4, 2004.

- > *...not something Microsoft ITSELF would*
- > *feel comfortable doing. I'd think many users would appreciate having the*
- > *virus quarantined or delete as soon as it appears to the system.*

The email has to be downloaded anyway, either way. The same definitions are in place, whether the program is set to scan incoming email, or just for on access scanning. If the mail scanner catches it, on access would have caught it had it got that far. If the mail scanner fails to catch it, on access will fail to catch it.

If the virus is too new for your definitions, mail scan will let it through; and some users, believing that NAV would have caught it, probably would run it! If the virus would be caught by your mail scan, it will be caught by your on access scan.

FWIW, on access will be invoked whenever an infected file in the definitions is manipulated; whether by the user, or the system. I know that for a fact, because NAV kept interfering with F-Prot for DOS. Mercury Mail invokes F-Prot for DOS as part of its AV Policy. Mercury Mail first writes the message to a scratch folder, then calls F-Prot for DOS. Alas, the first time I got a real-world virus infected email, it made it to the Inbox. MM wrote the message to disk, and NAV on access cleaned it. This deleted files that MM was monitoring, and MM timed out with no AV response; defaulted to

microsoft.public.security.virus: Re: Is this some sort of virus?

delivering the infected email. The interference has been corrected, by telling NAV on access to ignore the Mercury Mail scratch folder. But the point is, if the AV program is going to catch an infection at all, on access will catch it as easily as mail scan; without the problems that mail scan may cause otherwise.

In any case, the problem which caused the advice to turn off email virus scanning seems to have been fixed, at least so far as Symantec + MSOE is concerned, so I will withdraw my objection.

With one caveat; that the virus scanner failed to find a virus in an incoming email does not prove that the message is "clean". I received an email with the Bagle (Symantec's "W32.Beagle.J@mm") which cleared several layers of scan (ISP, local server + F-Prot for DOS, and NAV 2003 on access scan) on definitions only one day old. The latest crop of viruses were being released so fast that some AV vendors released two definition updates within a 24-hour period! Negative result do not mean the attachment is not viral!

--

Norman

~Win dain a lotica, En vai tu ri, Si lo ta
~Fin dein a loluca, En dragu a sei lain
~Vi fa-ru les shutai am, En riga-lint