Does my Antivirus Program Need an E-mail Scanner?

By Robert Spotswood

1. Short answer: No, unless you are running an e-mail server.

To understand why, you need to understand some basic facts about malware and how it works. All malware, be it a virus, trojan, worm, spyware, rootkit, adware, or any combination of them has one rule it must obey: It must be executed by something on your computer in order to infect you.

That something is usually the operating system (OS), most often Windows, although Macs are not as immune as Apple would like you to believe. The something can also be another program on your computer. Some examples include Office Suites, Adobe Reader, Adobe Flash, Outlook, Internet Explorer, as well as some others. However, the goal in today's malware world is to reach the OS. If one of the other programs is used, it's primarily as a doorway to the OS, i.e. download it, then get the OS to execute the file downloaded.

Unless and until a piece of malware is executed, even if it's sitting on your hard drive, or in your inbox, it can't do a thing. It's harmless, inert, and can be deleted at will. If the malware attempts to execute, your antivirus resident shield, if it detects the malware, will block it, protecting you from being infected.

Every antivirus product I've ever worked with that has an e-mail scanner has only one signature database. This database, and heuristics engine if present, is the same exact database used by the resident shield. So if the e-mail scanner would detect the malware, so will the resident shield. If the resident shield would miss the malware, so will the e-mail scanner.

So you have a situation where the e-mail scanner will detect anything that the resident shield will also detect. But if the resident shield detects the malware, then the malware can't execute. If the malware can't execute, the malware can't infect you. So having an e-mail scanner offers no additional protection.

In addition, distributing malware via e-mail is very rare today. Every decent e-mail provider out there today will scan your e-mails for malware and will reject/silently drop any messages found with malware attached. There a few instances where malware authors have attempted to get around this by encrypting the malware with a password and sending the password to decrypt it in the body of the message. But even in those cases, the e-mail scanner is useless because it can't decrypt the message to check it.

What malware that is "distributed" via e-mail takes the form of a message with a link to website, where the malware really is. Open the link, and it will most likely try to use a browser exploit to automatically download and install the malware. But since the malware isn't in the actual e-mail message, the e-mail scanner can't detect it, but a resident shield can.

A minority of the websites the malware e-mail will take you to don't use browser exploits, but throw up scary looking error screens designed to trick you into clicking on what they want to download and execute the malware. Again, no malware is in the e-mail message itself, so the e-mail scanner can't protect you.

Antivirus companies include e-mail scanners because, for a time, e-mail was the chief way of distributing malware. Having an e-mail scanner made people feel safer, even though it offered no additional protection. But making people feel safer helped sell more products. In the end, an e-mail scanner, unless you're running a mail server, is all about marketing, not security.

2. *The Down Side to E-mail Scanners*

At this point, you may be thinking, "Well even if the e-mail scanner doesn't protect me, at least it can't hurt me, right?"

[buzzer] **Wrong**. There are at least two problems that can be CAUSED by e-mail scanners. First, and this is one your author has seen multiple times, sometimes spam can confuse the e-mail scanner. In every case I've seen, the e-mail scanner will effectively block the downloading of all your e-mail until you disable the scanner. I suppose it's possible for an innocent message to do this as well, although I have yet to see this.

The other problem I have not witnessed personally, but have seen several reports of, is the e-mail scanner can corrupt your inbox, causing you to lose all your e-mails. Sometimes the corruption can be repaired, but sometimes it can't. This is rare thankfully.

3. *Doesn't scanning outgoing e-mails at least help protect my friends and family?*

No. First, as mentioned above, very few malware programs are transmitted by e-mail today. It's rather unlikely your infected computer will be sending any malware laden e-mails.

Second, if your computer is infected, then your antivirus scanner is already not detecting the malware, so it won't suddenly start detecting it in the outgoing messages. In all likelihood, your antivirus software has been crippled/disabled by the infection so it appears to be running, but it's not, so it won't detect any malware in any outgoing messages.

4. Conclusion

E-mail scanners are marketing tools and checklist items, not a good security tool. Having one adds nothing to your computer's security. However, if your antivirus program does include one, leave it enabled though. Disabling it will change the icon in your system tray to the "something is wrong" icon. This can mask a real problem.